

ED 354 314

CE 063 003

TITLE National Crime Information Center Mandatory Minimum Standards Curriculum for Full Access Terminal Operators. Volume One--Administrative Issues, Policy and the Interstate Identification Index.

INSTITUTION Federal Bureau of Investigation, Washington, DC. National Crime Information Center.

PUB DATE 92

NOTE 575p.; For volume 2, see CE 063 004. Some photocopied materials may be marginally legible.

AVAILABLE FROM Federal Bureau of Investigation, Criminal Justice Information Services Division, Training Section, Washington, DC 20535.

PUB TYPE Guides - Classroom Use - Teaching Guides (For Teacher) (052)

EDRS PRICE MF02/PC23 Plus Postage.

DESCRIPTORS Competency Based Education; *Computers; Computer Science; *Crime; Criminal Law; Criterion Referenced Tests; Curriculum Guides; Information Centers; Information Dissemination; *Information Networks; *Information Processing; Information Science Education; *Information Systems; Instructional Materials; Job Training; Law Enforcement; Lesson Plans; Online Systems; Postsecondary Education; Standards

IDENTIFIERS *Computer Related Occupations; *National Crime Information Center

ABSTRACT

This document is the first volume of a two-volume set of lesson plans which together make up a complete training package for full-service terminal operators. The lesson plans are designed to ensure that a state's National Crime Information Center (NCIC) training program meets Advisory Policy Board standards. (NCIC is a nationwide computerized information system serving local, state, and federal criminal justice agencies.) This volume contains lesson plans for seven areas of instruction: system history, shared management concept, hit confirmation, validation, system security, standards and sanctions, and interstate identification index. An introductory page to each area of instruction lists title, time allotted, target group, and method of instruction. The lesson plans consist of a statement of goal and objectives, criterion test and test answers, a list of required materials, and a block of instructional content. Certain materials are provided: information sheets, bibliography, overhead transparency masters, and handouts. The volume also contains a separate section giving the NCIC Bylaws, lists of Advisory Policy Board and Regional Working Group Members, and other materials pertaining to NCIC operations. (YLB)

* Reproductions supplied by EDRS are the best that can be made *

* from the original document. *

ED354314

**National Crime Information Center
Mandatory Minimum Standards Curriculum
For
Full Access Terminal Operators**



**Volume One - Administrative Issues, Policy
And The Interstate Identification Index**

**System History
Shared Management Concept
Hit Confirmation
Validation
System Security
Standards And Sanctions
Interstate Identification Index**

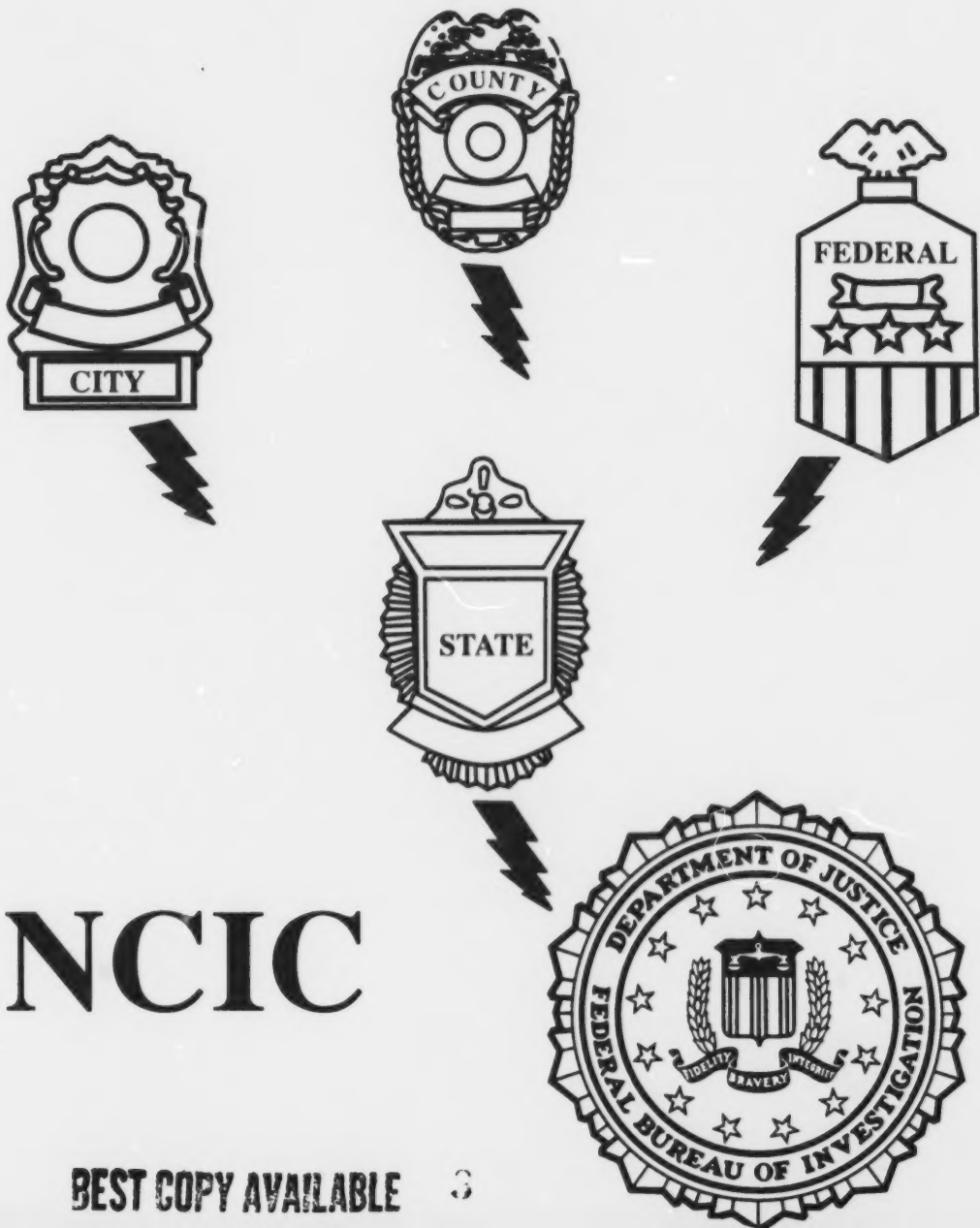
U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)

☒ This document has been reproduced as
received from the person or organization
originating it.
☐ Minor changes have been made to improve
reproduction quality.

• Points of view or opinions stated in this docu-
ment do not necessarily represent official
OERI position or policy.

CE063003

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: SYSTEM HISTORY



Federal Bureau of Investigation

Washington, DC 20535

October 19, 1992

TO: ALL CONTROL TERMINAL OFFICERS (CTOs) AND FEDERAL SERVICE COORDINATORS (FSCs)

Pursuant to the decision by the Advisory Policy Board to establish a "Mandatory Minimum Curriculum for Full-Service Terminal Operators," the FBI Criminal Justice Information Services (CJIS) Division's training staff has produced a collection of comprehensive lesson plans. Enclosed for your use is a set of lesson plans which are designed to ensure that your state NCIC training Program meets these standards.

This set of lesson plans encompasses all mandatory curriculum topics delineated by the Advisory Policy Board. The lesson plans create a complete training package for full-service terminal operators. Individual lesson plans may be used for "less than full access" operator training. Criteria for specific computer transactions, i.e., inquiry, locate, entry, modification, clear, and cancellation may be easily extracted from all "Hot File" lesson plans. For example, inquiry sections from all "Hot File" lesson plans can be used to instruct inquiry-only terminal operators.

Use of these lesson plans in your state training curriculum is optional. However, if audits have revealed problems in system usage attributed to training or you would like to include these in your training curriculum to ensure meeting Advisory Policy Board standards, we recommend and encourage the use of these lesson plans.

If you have any questions regarding these lesson plans or would like assistance from the CJIS Division's training staff in implementing these lesson plans in your state, contact Robert L. McFall at (202) 324-2615.

Sincerely yours,

Robert L. McFall
Acting Chief
Training Section
Criminal Justice Information
Services Division



Enclosure

TITLE OF INSTRUCTION:

System History

TIME ALLOTTED:

30 Minutes

TARGET GROUP:

Full Access Terminal Operators

INSTRUCTOR:

METHOD OF INSTRUCTION:

Lecture, Overhead Transparencies,
and Video Tape Presentations

DATE:

July 1, 1992

7/1/92

SH-11

PREFACE

The System History lesson plan is divided into seven parts. Below is an explanation of each part. Please review this section prior to instruction.

I. INTRODUCTION

This is a brief statement that is intended to obtain the interest of the trainee.

II. DEFINITION OF NCIC

This section defines the National Crime Information Center (NCIC) and describes its goal.

III. THE NCIC NETWORK

This section describes the NCIC computer system.

IV. PRIOR TO NCIC

This section describes how the idea of NCIC was conceived and what the law enforcement community had to do in order to receive information concerning wanted persons, missing persons, and stolen property.

V. THE CURRENT NCIC SYSTEM

This section lists the files that are currently available in NCIC and identifies the number of authorized user agencies, records in the system, and average number of transactions made against the system per day.

Refer to the NCIC Hot Files Lesson Plans for detailed information regarding the specific file.

VI. THE FUTURE NCIC SYSTEM

This section describes the planned system enhancements for the future NCIC system called NCIC 2000.

VII. CONCLUSION

This section highlights the important points to remember that are associated with the NCIC system.

**NCIC SYSTEM HISTORY LESSON PLAN
TABLE OF CONTENTS**

	PAGE
STATEMENT OF GOAL AND OBJECTIVES	SH-1
CRITERION TEST	SH-2
CRITERION TEST ANSWERS	SH-4
ITEMS AND MATERIALS	SH-6
INTRODUCTION	SH-7
DEFINITION OF NCIC	SH-8
THE NCIC NETWORK	SH-10
PRIOR TO NCIC	SH-11
THE CURRENT NCIC SYSTEM	SH-12
THE FUTURE NCIC SYSTEM	SH-14
CONCLUSION	SH-16
BIBLIOGRAPHY	SH-17

STATEMENT OF GOAL AND OBJECTIVES

Instructional Goal:

To describe to the terminal operator the development, current status, and planned system enhancements of the NCIC System.

Instructional Objectives:

At the conclusion of this block of instruction, the operator will be able to:

- 1) Define NCIC and know when it became operational.
- 2) State the goal of NCIC.
- 3) Identify the users who have access to NCIC.
- 4) List the 14 NCIC files.
- 5) Describe the major system enhancements under the new system, NCIC 2000.

CRITERION TEST

DEFINITION OF NCIC

1. Define NCIC.
2. Describe the goal of NCIC.
3. NCIC became operational on January 27, 1966.
 - a. True
 - b. False

THE NCIC NETWORK

1. The _____ is responsible for the complete operation of the NCIC computer.
2. From the following list, select the best answer that describes the location of the main NCIC computer:
 - a. Arizona DPS, Phoenix, AZ
 - b. FBI Headquarters, Washington, D.C.
 - c. RCMP Headquarters, Canada
 - d. INTERPOL Headquarters, France
3. NCIC serves _____ agencies in the 50 states, the District of Columbia, _____, _____, and _____.

PRIOR TO NCIC

1. The FBI, in conjunction with the _____ recognized that a computerized index of information could benefit criminal justice agencies.

THE CURRENT NCIC SYSTEM

1. List at least six NCIC Files.

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____

THE FUTURE NCIC SYSTEM

1. NCIC is being redesigned to provide advanced and expanded _____ and greater _____.
2. The differences between NCIC and the future system, NCIC 2000, will be:
 - a. Expanded existing fields
 - b. New fields
 - c. New transactions
 - d. All of the above

CRITERION TEST ANSWERS

DEFINITION OF NCIC

1. NCIC is a nationwide, computerized information system established to serve all criminal justice agencies on a local, state, and Federal level.
2. The goal of NCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of timely and accurate documented criminal justice information.
3. False. NCIC became operational on January 27, 1967.

THE NCIC NETWORK

1. The FBI is responsible for the complete operation of the NCIC computer.
2. b. The main NCIC computer is located at FBI Headquarters, Washington, D.C.
3. NCIC serves criminal justice agencies in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, and Canada.

PRIOR TO NCIC

1. The FBI, in conjunction with the International Association of Chiefs of Police (IACP) recognized that a computerized index of information could benefit criminal justice agencies.

THE CURRENT NCIC SYSTEM

1. The NCIC Files are:
 - a. Vehicle
 - b. License Plate
 - c. Boat
 - d. Gun
 - e. Article
 - f. Securities
 - g. Wanted Person
 - h. Missing Person
 - i. Unidentified Person
 - j. U.S. Secret Service Protective
 - k. Interstate Identification Index
 - l. Originating Agency Identifier (ORI)
 - m. Foreign Fugitive
 - n. Bureau of Alcohol, Tobacco and Firearms (ATF) Violent Felon

THE FUTURE NCIC SYSTEM

1. NCIC is being redesigned to provide advanced and expanded functionality and greater capabilities.
2. d. All of the above. The differences between NCIC and the future system, NCIC 2000, will be: expanded existing fields:
new fields: and new transactions.

7/1/92

SH-5

ITEMS AND MATERIALS

Overhead Transparencies, Overhead Projector, Screen,
VCR, and Monitor

Video Tapes: "NCIC Overview"
"NCIC/ATF Violent Felon File"
"NCIC 2000"

OVERHEAD TRANSPARENCIES (OH):

SH-OH #1	National Crime Information Center - System History
SH-OH #2	Definition of NCIC
SH-OH #3	NCIC Network Map
SH-OH #4	Before NCIC
SH-OH #5	Current NCIC System Information Bases
SH-OH #6	After NCIC
SH-OH #7	Mobile Digital Terminals (MDTs)
SH-OH #8	NCIC 2000
SH-OH #9	Differences Between NCIC and NCIC 2000
SH-OH #10	Image Transmission

HANDOUT MATERIALS (HD):

SH-HD #1	NCIC File Reference Card
SH-HD #2	Interstate Identification Index (III) - A Summary
SH-HD #3	"NCIC/Law Enforcement System Is Getting A Major Facelift"
SH-HD #4	"NCIC 2000: Technology Adds A New Weapon To Law Enforcement Arsenal"
SH-HD #5	"NCIC 2000"

I. INTRODUCTION

THIS 30-MINUTE BLOCK OF INSTRUCTION HAS BEEN DESIGNED TO INFORM THE TERMINAL OPERATOR OF THE DEVELOPMENT, CURRENT STATUS, AND PLANNED SYSTEM ENHANCEMENTS OF THE NCIC SYSTEM.

THE INSTRUCTOR SHOULD WELCOME AND INTRODUCE SELF TO THE GROUP; EXPLAIN COURSE GOAL AND OBJECTIVES; REVIEW AND DISTRIBUTE HANDOUT MATERIALS.

The National Crime Information Center, more commonly known as NCIC, has been in existence for over 25 years providing the criminal justice community with valuable information needed to carry out its duties.

NCIC has come a long way. As criminals devise new and more complex ways to elude law enforcement officers, NCIC must continue to keep pace.

The information presented in this lesson plan will include the history of the NCIC computer system and will aid in understanding the benefits derived from using the information in this valuable system.

References

IO = Instructional
Objective

OH = Overhead
Transparency

HD = Handout
Material

OH #1

II. DEFINITION OF NCIC

NCIC is defined as a nationwide, computerized information system established to serve all criminal justice agencies on a local, state, and Federal level. On January 27, 1967, NCIC became operational.

IO #1

OH #2

The goal of NCIC is to help the criminal justice community perform its duties; to provide and maintain a computerized filing system of timely and accurate documented criminal justice information; and to enhance officer safety.

IO #2

NCIC can best be described as a large automated "file cabinet" of information concerning crimes and criminals of nationwide interest, stolen property information and a locator-type file for missing* and unidentified persons.

INSTRUCTOR'S NOTE: * THE MISSING PERSON FILE HAS NO CONNECTION WITH THE CRIMINAL DATA STORED IN NCIC AND IS USED ALMOST EXCLUSIVELY BY STATE AND LOCAL CRIMINAL JUSTICE AGENCIES TO ASSIST IN THE LOCATION OF MISSING PERSONS.

The information stored in NCIC is organized into computer files which contain data on:

- Stolen Vehicles and/or Parts
- Stolen License Plates
- Stolen Articles
- Stolen Boats
- Stolen and Recovered Guns
- Stolen and Counterfeit Securities

- Extraditable Wanted Persons (including individuals wanted by other countries)
- Missing Persons
- Unidentified Persons, i.e., unidentified living and deceased; body parts
- Individuals being monitored by the U.S. Secret Service
- Originating Agency Identifier (ORI) Agency Information
- Criminal History Records
- Violent Felons who are of interest to the Bureau of Alcohol, Tobacco and Firearms

7/1/92

SH-9 17

III. THE NCIC NETWORK

- A. The FBI, as manager of the system, is responsible for the complete operation of the NCIC computer. The computer is located at FBI Headquarters in Washington, D.C. The FBI is responsible for all programming and personnel costs associated with the NCIC computer.
- B. NCIC provides virtually uninterrupted service 24 hours a day, 7 days a week.
- C. NCIC serves criminal justice agencies in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, and Canada. Connecting terminals are located throughout the country in police departments, sheriff's offices, state police facilities, Federal law enforcement agencies, and other criminal justice agencies.
- D. Under the shared-management concept, each agency accesses NCIC through their state system.

**INSTRUCTOR'S NOTE: REFER TO SHARED-MANAGEMENT
CONCEPT LESSON PLAN FOR FURTHER DETAILS.**

OH #3
LEAVE ON
PROJECTOR

IO #3

IV. PRIOR TO NCIC

OH #4

- A. Before NCIC was developed, a police officer would radio a terminal operator who would perform a manual record check. If the terminal operator found no record, then a state or nationwide all-points broadcast would be sent to determine if further information could be obtained.
- B. The idea of NCIC was conceived in the early 1960s as a result of law enforcement's growing need for vital information in a timely manner. The FBI, in conjunction with the International Association of Chiefs of Police, recognized that a computerized index of information could benefit criminal justice agencies.

V. THE CURRENT NCIC SYSTEM

A. In the initial stages of NCIC, there were only 15 criminal justice agencies tied to the NCIC network and five NCIC Files (Article, Vehicle, License Plate, Wanted Person, and Gun) which contained less than 21,000 active records. As of March 1, 1992, there were over 70,000 authorized user agencies. Nine files have been added to the system since the original five were brought on-line: Securities, Boat, Missing Person, Unidentified Person, U.S. Secret Service Protective, Interstate Identification Index*, Originating Agency Identifier, Foreign Fugitive, and Bureau of Alcohol, Tobacco and Firearms (ATF) Violent Felon. Authorized users of the system may inquire, enter, locate, modify, clear, or cancel records in NCIC**.

INSTRUCTOR'S NOTES: CHECK WITH YOUR STATE CTA CONCERNING FILES MAINTAINED AT THE STATE LEVEL. REFER TO HANDOUT MATERIALS THAT PERTAIN TO THE NCIC FILES. ALSO, FOR DETAILED INFORMATION REGARDING AN NCIC HOT FILE, REFER TO THAT LESSON PLAN.

*** THE INTERSTATE IDENTIFICATION INDEX IS CURRENTLY MAINTAINED BY THE FBI'S IDENTIFICATION DIVISION.**

**** REFER TO THE NCIC HOT FILES LESSON PLANS FOR A DEFINITION OF EACH TYPE OF TRANSACTION; INFORM STUDENTS THAT ONLY CERTAIN TRANSACTIONS CAN BE PERFORMED ON THE FOLLOWING FILES: U.S. SECRET SERVICE PROTECTIVE, INTERSTATE**

IO #4

OH #5

HD #1-2

**IDENTIFICATION INDEX, FOREIGN FUGITIVE, AND
ATF VIOLENT FELON FILES; CHECK WITH YOUR CTA
OR FSC TO DETERMINE YOUR AUTHORIZED LEVEL OF
ACCESS.**

B. As of March 1, 1992, there were over 20 million records in NCIC. Approximately 15 million of those records are criminal history records maintained in the Interstate Identification Index (III). NCIC processes, on the average, over a million transactions per day.

C. The information contained in NCIC can be provided to criminal justice personnel in a matter of seconds. A terminal operator can now respond quickly to information requests from all authorized personnel.

OH #6

D. NCIC may also be accessed through the use of mobile digital terminals or MDTs (vehicle-mounted terminals) by some departments. MDTs provide the law enforcement officer direct access to the state and NCIC computer without relaying the information to and from a terminal operator. This saves time and eliminates the possibility of errors being made due to poor radio transmissions.

OH #7

**INSTRUCTOR'S NOTE: SHOW "NCIC OVERVIEW" AND
"NCIC/ATF VIOLENT FELON FILE" VIDEOS (PLAYING
TIMES: 6:19 MINUTES/10:15 MINUTES).**

VI. THE FUTURE NCIC SYSTEM

- A. The current NCIC System is unable to keep pace with the ever-increasing user demand for enhancements and new applications.
- B. NCIC is being redesigned to provide advanced and expanded functionality and greater capabilities. Existing capabilities will remain unchanged. The differences between NCIC and the future system, NCIC 2000, will be expanded existing fields, new fields, and new transactions. OH #8
OH #9
- C. New features of the system will include, but are not limited to: IO #5
1. The technology now exists to transmit fingerprints and photographs (Image Transmission) between national, regional, local, and even mobile locations. In the future, it will be possible to electronically scan and compare the fingerprint of a suspect from a patrol car and within seconds obtain a positive identification. OH #10
 2. It will be possible to link records that are logically related so that a single

inquiry retrieves all information associated with the inquiry, e.g., linking information on wanted persons with information on stolen guns.

3. An "intelligent workstation", once developed, will provide a terminal with built-in help files, editing, and security features.
4. Users will be able to submit inquiries and receive responses from other external databases outside of NCIC such as the Canadian Police Information Centre (CPIC)* and SENTRY*.

INSTRUCTOR'S NOTE: *THE CANADIAN POLICE INFORMATION CENTRE (CPIC) SYSTEM, LOCATED AT THE ROYAL CANADIAN MOUNTED POLICE HEADQUARTERS IN OTTAWA, ONTARIO, PROVIDES ACCESS TO THE CANADIAN VEHICLE AND PERSON FILES.

SENTRY, MAINTAINED BY THE FEDERAL BUREAU OF PRISONS, PROVIDES INFORMATION ON PERSONS CURRENTLY INCARCERATED IN U.S. FEDERAL PRISONS.

SHOW "NCIC 2000" VIDEO (PLAYING TIME: 14:00 MINUTES). REFER TO HANDOUT MATERIALS THAT PERTAIN TO NCIC 2000.

HD #3-5

VII. CONCLUSION

In summary, NCIC became operational on January 27, 1967, and has supported law enforcement for more than two decades.

As criminals devise new and more complex ways to elude law enforcement, NCIC continues to keep pace with added new files and major enhancements to improve its capabilities.

It is important to remember:

1. NCIC is a nationwide, computerized information system established to serve all criminal justice agencies on a local, state, and Federal level.
2. NCIC serves criminal justice agencies in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, and Canada.
3. There are 14 NCIC files: Vehicle; License Plate; Boat; Gun; Article; Securities; Wanted Person; Missing Person; Unidentified Person; U.S. Secret Service Protective; Interstate Identification Index; Originating Agency Identifier; Foreign Fugitive; and the Bureau of Alcohol, Tobacco and Firearms (ATF) Violent Felon.
4. NCIC, when redesigned, will provide advanced and expanded functionality and greater capabilities to its users.

The information presented in this lesson plan will enhance the knowledge of the terminal operator on the NCIC System.

BIBLIOGRAPHY

- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC Newsletter. pp. 1,4. "NCIC Celebrates Twentieth Anniversary." 87-1.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC Newsletter. p. 1. "We've Come A Long Way." 88-1.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC Newsletter. pp. 5-6. "NCIC 2000." 90-1.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC Operating Manual. Introduction. Section 1, pp. Intro 1 - 2. May 31, 1989. Revision 55.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. "NCIC/ATF Violent Felon File" Video. January, 1992. 10:15 Minutes.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. "NCIC Overview" Video. March, 1990. 6:19 Minutes.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. "NCIC 2000" Video. April, 1991. 14:00 Minutes.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC 2000 User Requirements Concepts. Concept No. 246, p. 279. April, 1987.
- Mikelskas, Dr. Robert A. Executive Summary - National Crime Information Center 2000 Project - Phase I Study. The Mitre Corporation. March, 1990.
- Royal Canadian Mounted Police. Canadian Police Information Centre. Ottawa, Ontario. CPIC Reference Manual. Introduction to CPIC. Chapter I.1, pp. I-1-1 - 1-4. September, 1989. Revision 26.

U.S. Department of Justice. Federal Bureau of Investigation.
Washington, D.C. Make NCIC Work For You. Revised
February, 1983.

U.S. Department of Justice. Federal Bureau of Investigation.
Washington, D.C. National Crime Information Center -
The Investigative Tool: A Guide to the Use and Benefits
of NCIC. March, 1982.

U.S. Department of Justice. Federal Bureau of Investigation.
Washington, D.C. National Crime Information Center -
The Investigative Tool: A Guide to the Use and Benefits
of NCIC. June, 1986.

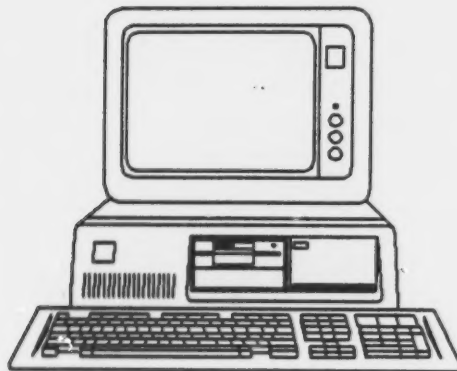
OVERHEAD TRANSPARENCIES

SH-OH #1-10

NCIC System History Lesson Plan

7/1/92

NATIONAL CRIME INFORMATION CENTER
SYSTEM HISTORY



7/1/92

SH-OH #1

DEFINITION OF NCIC

**NCIC IS DEFINED AS A NATIONWIDE, COMPUTERIZED
INFORMATION SYSTEM ESTABLISHED TO SERVE ALL
CRIMINAL JUSTICE AGENCIES ON A LOCAL, STATE,
AND FEDERAL LEVEL.**

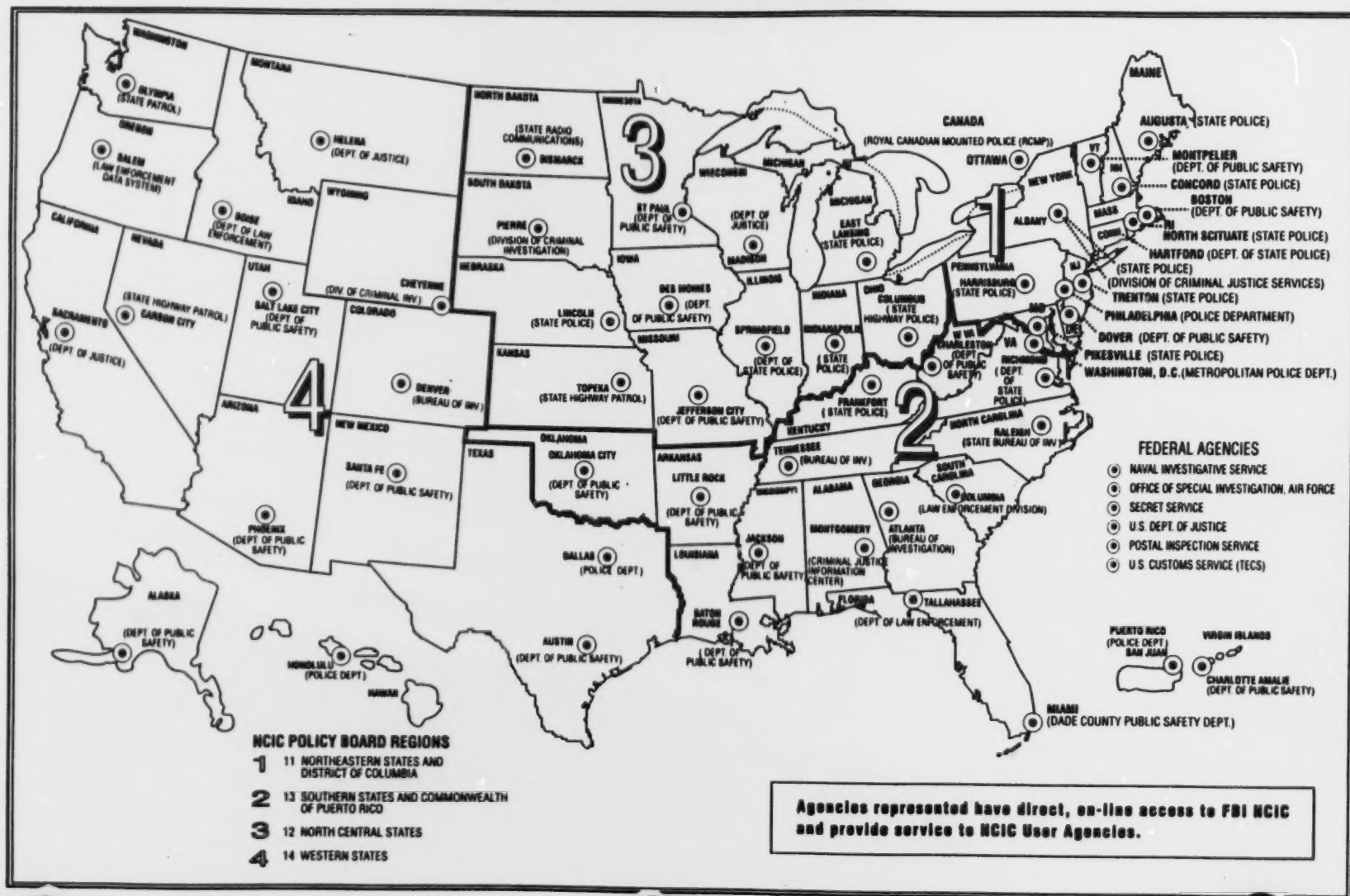
City

Federal——State——FBI NCIC

County



NCIC NETWORK



BEFORE NCIC

Patrol Car————Dispatcher

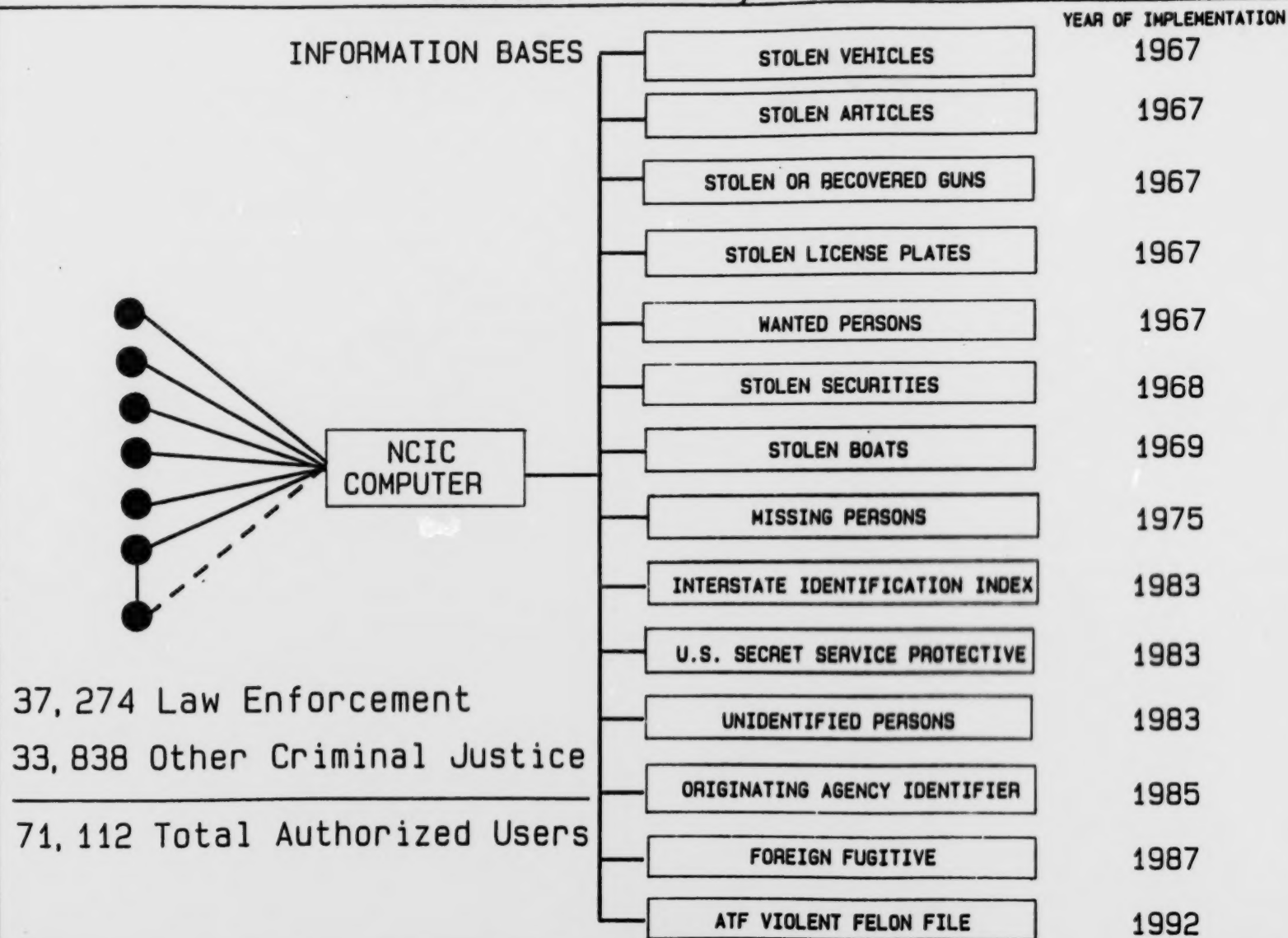
Dispatcher————Check Manual Local Records (No Record)

Dispatcher————Send Teletype (State APB/National APB)

7/1/92

SH-OH #4

Current NCIC System



AFTER NCIC

Patrol Car————Dispatcher

**Dispatcher/Terminal Operator————Check Local/State
Automated Files/NCIC**

7/1/92

SH-OH #6

MOBILE DIGITAL TERMINALS (MDTs)



Patrol Car-----State/Local Automated Files-----NCIC

7/1/92

SH-OH #7



**NCIC
2000**



DIFFERENCES BETWEEN NCIC AND NCIC 2000

- Expanded existing fields
- New Fields
- New Transactions

IMAGE
TRANSMISSION

7/1/92

SH-OH #10

HANDOUT MATERIAL

SH-HD #1-5

NCIC System History Lesson Plan

NCIC FILE REFERENCE CARD

AUTHORITY FOR MAINTENANCE OF THE SYSTEM

The System is established and maintained in accordance with Title 28, United States Code, Section 534 and Title 28 of the Code of Federal Regulations--Judicial Administration, Chapter I--Department of Justice (Order No. 601-75) Part 20--Criminal Justice Information Systems. Public Law 92-544 (86 Stat. 1115), Executive Order 10450, Public Law 94-29 (89 Stat. 97) Security Acts Amendments of 1975.

2. CATEGORIES OF USERS

Data in NCIC files is exchanged with and for the official use of criminal justice officials of Federal, state, and local governments in the 50 states, the District of Columbia, Puerto Rico, U.S. possessions and U.S. territories, and Canada.

3. THE THIRTEEN NCIC FILES

Article

- Records for any item valued at \$500 or more having a unique manufacturer-assigned serial number and/or owner-applied number.
- Records for any item, regardless of value, if aggregate value of all property taken in one theft exceeds \$5,000 and having a unique manufacturer-assigned serial number and/or owner-applied number.
- Records for any item, regardless of value, having a unique manufacturer-assigned serial number and/or owner-applied number if interstate movement is indicated, or the stolen item is a lead in a more serious crime.

Boat File

- Records for stolen boats, boat trailers, or boat parts.

Foreign Fugitive File

- Records for persons wanted by another country for a crime that would be a felony if it were committed in the United States.
- Wanting country must be a signatory to an extradition treaty/convention with the U.S.

Gun File

- Records for stolen weapons.
- Records for recovered, (abandoned, seized, or found) weapons for which the owner is not known.

Interstate Identification Index (III)

- Criminal history information provided by indexing record identifiers such as name, physical description, identifying numbers, and fingerprint classifications as well as the name of the agency that maintains the criminal history record.

License Plate File

- Records for stolen license plates.

Missing Person File

- Records for persons of any age who are missing and under proven physical/mental disability or are senile, thereby subjecting himself/herself or others to personal and immediate danger.
- Records for persons of any age who are missing under circumstances indicating that his/her physical safety may be in danger.
- Records for persons of any age who are missing under circumstances indicating that his/her disappearance may not have been voluntary.
- Records for persons who are missing and declared unemancipated as defined by the laws of his/her state of residence and do not meet any of the above entry criteria.
- Records for persons of any age who are missing after a catastrophe.

Originating Agency Identifier (ORI) File

- Records for agency information on any criminal justice agency that has been assigned an NCIC ORI for the purpose of accessing the NCIC System.

Securities File

- Records for serially numbered stolen, embezzled, or counterfeit securities, e.g., currency and documents or certificates which are considered evidence of debt, or ownership of property, or documents which represent subscription rights. Also, warehouse receipts, traveler's checks, money orders, savings certificates, and interest coupons on stocks and bonds.

Unidentified Person File

- Records for unidentified deceased persons.
- Records for persons of any age who are living and unable to ascertain his/her identity.
- Records for unidentified catastrophe victims.
- Records for body parts.

U.S. Secret Service (USSS) Protective File

- Records for individuals who may pose a threat to the President and/or others afforded protection by the USSS as authorized by 18 USC 3056 and Public Law 90-331 as amended.

Vehicle File

- Records for stolen vehicles.
- Records for vehicles involved in the commission of a crime (felony vehicle).
- Records for stolen component parts.

Wanted Person File

- Records for individuals (including a juvenile who will be tried as an adult) for whom a Federal warrant is outstanding.
- Records for individuals (including a juvenile who will be tried as an adult) for whom a felony or serious misdemeanor warrant is outstanding.
- Records for probation and parole violators.
- Records for any juvenile offender may be entered for escapees, probation and parole absconders, and those juveniles charged with the commission of an act of delinquency.
- A temporary felony want may be entered when a law enforcement agency must take prompt action to apprehend a person who has committed, or there are reasonable grounds to believe has committed, a felony and who may flee across jurisdictional boundaries and a warrant cannot immediately be obtained.

4. RETRIEVABILITY

On-line access to data in NCIC is achieved by using the following search descriptors:

Article File

- Type (TYP) and serial number.
- TYP and owner-applied number (OAN).
- TYP, serial number, and OAN.
- NCIC Number (NIC).

Boat File

- Registration (RBO), document number (CGD).
- Hull serial number (BHN).
- OAN.
- LIC.
- VIN.
- or any combination of the above.
- NIC.

Foreign Fugitive, USSS Protective, and Wanted Person Files

- Name and at least one of the following numerical identifiers: date of birth (DOB), FBI Number, Social Security (SOC) Number, operator's license number, miscellaneous number (MNU) (Canadian Social Insurance Number, military serial number, passport number, Selective Service Number, Veterans' Administration claim number, etc.), originating agency case number (OCA).
- Name, DOB, sex, and race.
- License Plate number (LIC) and license plate state (LIS).
- Vehicle identification number (VIN).
- LIC only.
- NIC.

Gun File

- Serial number (SER), make (MAK), and caliber (CAL).
- SER and MAK.
- SER and CAL.
- SER only.
- NIC.

Interstate Identification Index

- Name, sex, race, and DOB.
- Name, sex, race, DOB, and either an MNU or SOC Number.
- Name and SOC Number, MNU, State Identification Number, or FBI Number.
- State Identification Number.
- FBI Number.

License Plate File

- LIC and LIS.
- LIC.
- NIC.

Missing Person File

- Name and any one or more of the following: DOB, FBI Number, MNU, SOC Number, operator's license number, LIC, VIN, and OCA.
- Name, DOB, sex, and race.
- LIC and LIS.
- VIN only.
- LIC only.
- Approximate age, sex, race, eye color, hair color, approximate height, and approximate weight.
- Entry of an Unidentified Person record.
- NIC.

Originating Agency Identifier (ORI) File

- ORI

Securities File

- TYP, serial number, denomination of security.
- Name of owner of security.
- Name of owner of security and TYP, SOC Number, or OCA.
- SOC Number.
- NIC.

Unidentified Person File

- Body parts status.
- Age, sex, race, height, weight, eye color, and hair color.
- OCA Number.
- Entry of a Missing Person Record.
- NIC.

Vehicle File

- VIN.
- OAN*.
- SER*.
- LIC.
- LIC and LIS.
- LIS may be used in combination with any of the above
- NIC.

5. RETENTION

Unless otherwise removed or located, records will be retained in file as follows:

Article File -- Balance of the year entered plus one year.

Boat File -- Balance of the year entered plus four years. Records without a BHN or OAN remain in file for 90 days after entry.

Foreign Fugitive File -- Unlocated records remain in file indefinitely or until the originating agency clears/cancels the record.

Gun File -- Records are retained in file until the originating agency clears the record. Records on file as recovered weapons will remain in file for the balance of the year entered plus two years.

Interstate Identification Index -- Records are retained until the individual reaches the age of 80.

License Plate File -- Records remain in file for one year after the end of the plate's expiration year. Records for nonexpiring license plates remain in file for the year of entry plus four years.

Missing Person File -- Unlocated records remain in file indefinitely or until the originating agency clears the record.

Originating Agency Identifier File -- Records remain in file indefinitely. If an agency no longer qualifies for NCIC access, the ORI record is retired, keeping it in file in an inactive status.

Securities File -- Balance of the year entered plus four years, except records for traveler's checks and money orders which are retained for the balance of the year entered plus two years.

Unidentified Person File -- Records are retained for the remainder of the year of entry plus nine additional years.

U.S. Secret Service Protective File -- Records remain in file until action is taken by the USSS.

Vehicle File -- Felony vehicle records and records not containing a VIN or OAN will remain in file for 90 days after entry. Records containing a VIN or OAN and stolen part records containing an OAN or SER will remain in file for the year of entry plus four years. LIC data in a vehicle record is purged one year after the plate's expiration year except for nonexpiring license plates which remain until the entire record is purged.

Wanted Person File -- Unlocated records (adult and juvenile) remain in file indefinitely or until the originating agency clears/cancels the record. Temporary felony want records will be automatically removed from file after 48 hours.

*These identifiers apply to stolen part record inquiries.



U.S. Department of Justice
Federal Bureau of Investigation
National Crime Information Center (NCIC)

INTERSTATE IDENTIFICATION INDEX (III) A SUMMARY

Even though the III Program began in 1983, NCIC users continue to request information about the Program and its operations. This publication is intended to answer those questions most frequently asked.

WHAT RECORDS ARE IN III?

The criminal records of about 15 million people are available. These records represent all people born in 1956 or later with an FBI record, persons born prior to 1956 whose first arrest fingerprint card was submitted to the FBI in 1974 or later, and selected older records converted to the automated systems for certain fugitives and repeat offenders.

WHAT IS THE EXTENT OF STATE PARTICIPATION?

Twenty-two state agencies are responsible for providing about half of the available criminal records. Agencies in all states have direct access to the System.

HOW DO I MAKE A III INQUIRY?

If a person's FBI Number is known from a previous fingerprint identification, use it to make the III inquiry. Use of the FBI Number eliminates receiving multiple record responses.

WHAT RECORDS ARE NOT IN III?

There are no records for individuals who have been arrested but whose fingerprints were not sent to the FBI. Also, there are about 12 million older records that are in the FBI manual files only.

WHAT ABOUT FBI PARTICIPATION?

The FBI provides over six million records for Federal offenders and persons arrested in the 28 states not capable of providing their own criminal arrest data.

WHAT IF THE FBI NUMBER IS UNKNOWN?

If the FBI Number is unknown, the index records can be searched for a matching record by using the name, sex, race, and date of birth or Social Security Number. This type of inquiry may result in more than one matching record for persons with similar names and dates of birth.

NOTE: A positive identification can be made only by comparison of fingerprints. Professional judgement must be used to associate records with individuals based solely on names and descriptors.

Revised 10/10/91

HOW CAN I USE III TO OBTAIN THE ACTUAL CRIMINAL RECORD?

To request a criminal record, the subject's assigned FBI or State Identification Number must be used. These numbers may be obtained from local files when a previous fingerprint card was submitted, or they may be obtained by searching the Index. Criminal records are often received from the FBI and state files within 60 seconds of the request.

WHY NOT JUST REQUEST AN FBI IDENTIFICATION RECORD?

III record responses contain as much or more information than the FBI Identification records. Also, getting information via III is quicker. Since updates and expungements are being applied to the files on a continuous basis, we suggest you request another record each time one is needed. This will ensure that the information you have is up to date.

FOR WHAT PURPOSES CAN III BE USED?

III may be used for official criminal justice purposes, e.g., criminal investigation, risk assessment, bond setting, charging determination, sentencing, and criminal justice employment. Also, plans are being considered to use the System for responding to applicant fingerprint cards.

WHAT USES OF III ARE PROHIBITED?

Any noncriminal justice use of the records is generally prohibited. The only exception is when an applicant fingerprint card is identified with a record by the FBI or a state bureau of identification for an authorized purpose.

CAN I USE A FACSIMILE MACHINE TO TRANSMIT CRIMINAL HISTORY RECORDS?

Yes, providing that both agencies involved have an NCIC Originating Agency Identifier authorized to receive criminal history information. Not all facsimile machines are monitored continually, so it is important to notify the receiving agency by telephone prior to transmitting the information. This will ensure proper retrieval of information and serves to verify the authenticity of the receiving agency.

RECORD-PROVIDING STATES

Alaska
California
Colorado
Connecticut
Delaware
Florida
Georgia
Idaho

Michigan
Minnesota
Missouri
Montana
New Jersey
New York
North Carolina
Ohio

Oregon
Pennsylvania
South Carolina
Texas
Virginia
Wyoming

National Crime Information Center

Law Enforcement System is Getting a Major Face-lift

There will be a far-reaching effect on law enforcement officers at every level when the antiquated National Crime Information Center is modernized.

Donald A. Woodmancy

Don Woodmancy is an information systems consultant to government and a nationally published writer for the information technology industry.

The National Crime Information Center, universally known as NCIC, has been the mainstay of law enforcement for more than two decades. It was the first computer-based technological innovation to be widely used in police work.

But NCIC is growing old and tired. Both the hardware and the programming are old technology and the system is difficult to maintain or modify. As a result, its users - every police agency in the country - are unable to exploit new technology using the system.

The resolution for these problems is on the horizon. For the past several years, the FBI and a wide spectrum of systems users have been defining NCIC's replacement - NCIC-2000. When completed, NCIC-2000 will have a far reaching effect on law enforcement at all levels of government.

The current NCIC system is a collection of computer hardware, software and communications networks. It is a repository

for public record information relating to missing, unidentified and wanted persons, stolen license plates and vehicles, stolen firearms, securities and other stolen property with serial numbers.

Routine Use of NCIC

When a peace officer has cause to suspect a person, vehicle or serial numbered article, the officer can make a check through NCIC to determine if that person or article is wanted by police anywhere in the country. If there is a matching record in the system, NCIC returns a "hit" message. It is then the responsibility of the agency making the inquiry to verify the "hit" with the agency that originated the wanted status.

Peace officers at every level of government routinely use NCIC. The system contains more than 19 million records and averages more than 900,000 inquiries per day. Peak activity is well over one million inquiries per day.

NCIC is operated by the FBI. The NCIC network connects with state and regional law enforcement telecommunications networks through which inquiries are routed. These networks service the needs of almost every state and local peace officer in the country as well as those of many federal officers.

"Computer systems should be rebuilt or replaced about ev-

ery eight years to take advantage of new technology," said FBI Special Agent David Nemecek, NCIC chief. "NCIC came on line in 1967 and we are still using the original software."

Nemecek said that the original NCIC system works well, but is difficult to modify for emerging technology. The software is written in a first generation assembly language. The new system will be done in fourth and fifth generation higher level programming languages.

Most of NCIC-2000 is evolutionary. It will replicate and extend the existing capabilities. It will also provide the ability to more easily add functionality as technology changes.

"we had significant input from users and other stakeholders in the definition of NCIC-2000," Nemecek said. "Extensive surveys and interviews were conducted with users, civil libertarians, legislators and others."

From that input, concept proposals - more than 200 of them - were defined. After being reviewed in depth by the NCIC Advisory Policy Board, FBI management and others, the list was reduced to about 80 conceptual proposals. At the conclusion of the process, FBI Director William Sessions approved the remaining items, which form the basis for NCIC-2000 development.

Civil Rights Controversy

One area of controversy that surfaced during the definition phase concerned the extension of NCIC to provide intelligence and tracking of people suspected of involvement in drug dealing, terrorism, arson and murder. Although there was strong support from many of the law enforcement personnel involved in the planning effort, intelligence and tracking features did not make it into the final definition.

"Any national police telecommunications system is an inherent threat to the rights of Americans," said U.S. Rep. Don Edwards, San Jose, Calif. Edwards, chairman of the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee, has been actively involved in reviewing NCIC-2000.

"I am a strong supporter of NCIC, which is an important tool for law enforcement," he continued. His concern was that NCIC remain a fact-based record system and not be used for intelligence or tracking purposes.

Edwards and other civil liberties activists are especially pleased with some of the changes planned for NCIC. Since the current system matches descriptive record information with information supplied in the inquiry such as name, date of birth and serial numbers, it is possible to have mis-identifications.

It does not happen often, but when it does it can subject innocent people to inconvenience, arrest or even injury and death. Changes which reduce the proba-

bility of such errors are welcomed, according to Edwards.

The proposed changes fall into several categories. They include data quality, added data fields, enhanced functionality for existing applications, positive identification on inquiries and linkage to external databases. All of these changes have increased officer safety, greater police efficiency and effective use of computer and communications resources as their goal.

Intelligent Workstations

One of the primary data quality proposals is the creation of intelligent workstations for use by local agencies. These PC-based workstations would have the capability of formatting and editing input and inquiries. Some agencies already have this capability, but many now operate on teletype compatible terminals.

The standard workstation would be based on the 80386 processor and have a specifically defined configuration. Two versions of the workstation would be available - the second supporting graphics capability. In either case, standard software would be made available for use by state and local agencies.

These terminals will not only improve data accuracy and line utilization, but make training easier for data entry and inquiry operators. Currently, many data entry terminals require strictly formatted messages. The new screen formats will be menu driven and conversational so operators should become capable more quickly.

Other data quality propos-

als are to provide more descriptive error messages and a process for systematic periodic revalidation of records stored on the system.

Another set of proposals relate to adding data fields to existing files. Proposals include increasing the size of the field available for miscellaneous information, adding fields to for the warrant number in the wanted person file, adding a "caution flag" in the wanted and missing persons files and a field to enter the original offense code in the wanted person file.

Hit Confirmation

Another group of concepts are designed to enhance internal capabilities of the system. One would be to use NCIC to confirm "hits" with the originating agency (ORI). Currently when a "hit" is received, the agency with the suspect or items must telephone or teletype the ORI to confirm the wanted status. With this proposal, NCIC would generate a confirmation request when the hit is received.

Time and date stamps would be added to data records when entered to enhance internal control. There would also be the capability to add lost weapons to the file that now contains only stolen firearms.

A proposal would provide the telephone number of the ORI on each hit message. Another would provide the capability to store inquiries for some period of time after they were made. Then, as new data were entered in the system, these stored inquiries would be checked and if "hits"

were encountered, both the inquiring agency and the ORI would be notified.

Stolen vehicles can be used to illustrate this function. Frequently, police agencies contact - and in some cases - impound stolen vehicles before they have been reported as stolen and may hold them for days without discovering they are stolen. In cases where a vehicle was stopped and then released, police can be notified and possibly recontact the thief. This new proposal would enhance the system's ability to detect and report such situations.

The changes previously described are primarily evolutions of the existing system. There are another set of proposals that are more revolutionary and take advantage of emerging technology.

Image Technology

The most revolutionary of the changes involve image transmission technology. NCIC depends on matches for data supplied with the original entry and with the inquiry. Because suspects sometimes supply false names or identifications and because many names are common to hundred or thousands of people, mis-identifications and missed identifications are possible.

When they happen, persons, vehicles or articles that should be seized or not, or worse, innocent people are detained, arrested or injured. Image technology has the potential to minimize such situations. Photographs, fingerprints, drawings and other images can be trans-

mitted between national, regional, local and even mobile locations to aid positive identifications.

This capability has been successfully tested in Aurora Colo., and Santa Barbara, Calif., using one-of-a-kind equipment. According to Nemecek, no single vendor currently supports such capability. However, the FBI was able to locate various off-the-shelf products from a variety of sources to integrate it successfully.

Nemecek said that Aurora and Santa Barbara were selected for the test to demonstrate these capabilities in active jurisdictions and across long distances.

The test in Aurora was a 100 percent success, according to W. Gray Buckley, chief of Colorado's Crime Information Center in the Colorado Bureau of Investigation. "The technology is here now and it works," he said.

Buckley said that although it is feasible to use this technology in police cars now, he does not expect every police car to be equipped for many years, if ever. He does believe that some cars and many local stations will be equipped to receive and, in some cases, send images as the capability is made available in the NCIC system.

The test in Santa Barbara was also a success. Fred Wynbrandt, assistant director for the Division of Law Enforcement in the California Department of Justice, is enthusiastic about its potential.

"We had two objectives in the test," Wynbrandt said. "We wanted to test the feasibility of

the concept and we wanted input from local law enforcement. The quality of the images transmitted was good and the police really liked it."

The capability to transmit photographs was especially useful. Officers were able to confirm a person's identity. It was even possible to send photos of tattoos when needed.

While it is possible to send images of fingerprints from or to the field, it is not yet feasible to identify them except when the subject's identity is suspected.

One of the problems with such identification is the time required. The courts have exerted stringent limitations on the amount of time citizens may be detained for investigation. The FBI does not currently have the technology to scan and identify unknown prints within allowable time frames.

A test system is expected soon that may improve this situation, according to Nemecek. If it works as expected, it should be possible to scan the wanted and missing persons file of some 400,000 records. However, he does not believe the technology currently exists to scan the millions of criminal fingerprint records on file in the few minutes available.

Another concept proposed for more positive identification is to cross-reference suspects who have used stolen or false identification. With this feature, officers will have a better probability of identifying wanted persons and avoiding the arrest of innocent people whose identity has been

assumed by someone else.

Criminal Information Link

Another set of proposals relate to linkage of NCIC with other criminal information systems. Included would be a periodic comparison of the wanted and missing person file to the U. S. Bureau of Prisons file of incarcerated people. It is thought that many subjects in the wanted file are probably in prison for other crimes. This proposal will detect such situations, at least for federal prisoners.

A second linkage would be to the Canadian Police Information Center (CPIC). The United States and Canada share the longest unguarded border in the world. However, facilities do not exist for police in one country to make routine inquiries to the other country on persons, vehicles or property. This proposal provides a telecommunications link between the two systems for such inquiries.

The third linkage would be to the FBI's Criminal Records System, which would make authorized access to such records easier and promote more accurate data in the records system.

There are a variety of other technical proposals and concepts in the plan to enhance internal control and audits and to improve security for these sensitive databases. Some of these include the improvement of internal statistics, enhanced file search techniques and the use of artificial intelligence to improve data matching and reduce mis-identifications.

Planners are working to

cushion the impact of these changes on state and local government, but there will be an effect. According to Nemecek, users will be able to use the new system without changing their systems for some period of time. However, to make use of the new features and functions, they will need to make software and, in many cases, hardware changes.

That burden will fall most heavily on the states since the direct connection to NCIC is from the state criminal justice computer systems. However, there will also be costs to regional and local governments. In many cases, programming and hardware changes will be necessary interfaces to the state systems.

There will certainly be expenses to local and regional agencies to equip their stations and vehicles with either intelligent terminals, image equipment or both. Substantial costs will also be incurred to train police personnel to use this equipment. Planners believe that these costs will be offset by improvements in officer safety and effectiveness and in reduced civil liability for the results of mis-identification.

There will also be a significant effect on law enforcement techniques and operations. It is not unreasonable to believe that image transfer technology will exert a change on police procedure as great as the widespread use of mobile radio in the 1930's and 40's or the introduction of NCIC in the 60's.

With widespread consensus on what NCIC-2000 should be,

funding is now the central issue. Nemecek estimates the enhanced system will cost the FBI about \$75 million over a five- or six-year period. With the deficit reduction efforts, it has been difficult to obtain program approval for the new system.

Buckley, who is current chairman of the NCIC Advisory Policy Board, and Wynbrandt, who is its former chairman, feel the political outlook for funding is good. Rep. Edwards, whose subcommittee provides congressional oversight of the FBI, is a strong supporter of the program. He stated flatly that he is going to make sure it is funded.

While widespread availability of NCIC-2000 features is some years in the future, its potential users are enthusiastic and anxious. "NCIC-2000 is a magnificent step into the future and a blueprint for making tremendous advances," Wynbrandt said.

On the Cutting Edge

NCIC 2000:

Technology Adds a New Weapon to Law Enforcement's Arsenal

By DAVID F. NEMECEK, Chief, National Crime Information Center, Federal Bureau of Investigation, Washington, D.C.

A law enforcement officer on routine patrol observes an out-of-state car exceeding the posted speed limit. While in pursuit, the officer radios the car's license plate number and state to his dispatcher, who keys in an inquiry to the regional and state computers. A further inquiry is transmitted to the National Crime Information Center (NCIC) at FBI headquarters in Washington, D.C. Within seconds, a "hit" is relayed by the dispatcher to the officer. Proceeding with the stop, the officer obtains the occupant's driver's license and the vehicle's registration papers and again radios the dispatcher, requesting two additional checks: one on the information from the registration papers and the other on the name, date of birth and physical description from the driver's license. Again, within a few seconds a negative response is relayed by the dispatcher to the officer. The officer returns the documents to the car's occupant and proceeds to execute a traffic citation for exceeding the speed limit. During this time, the officer asks some "routine" questions and keenly observes the violator's physical movements and emotional attitude as he responds. Nothing suspicious is observed, so the violator is given the traffic citation and sent on his way. Unfortunately, this traffic violator has an extensive criminal history on file under a different name, is using a forged license, has intentionally altered his physical appearance and is wanted in three states for brutal sex crimes.

In the foregoing scenario, did the officer err, or did the fugitive go free because of failure in the criminal justice system? The answer is neither of these. Consequently, a loophole exists whereby individuals who are fugitives from justice evade being positively identified and thus tied to their past unlawful actions. The actual number of incidents like the one above is not documented; however, such incidents are considered to be occurring more frequently as our society becomes more mobile and utilization of fraudulent identification increases.

With more than 16,000 city, county and state law enforcement agencies in the United States, the scope of the problem is significant. As an example, the California Highway Patrol makes over four million vehicle enforcement stops each year, during which about 152,000 arrests are made for causes ranging from driving under the influence of alcohol and/or drugs to homicide. But out of the remaining 3.8 million or so who were sent on their way, how many were undetected fugitives?

As most criminal justice practitioners are aware, NCIC was established by the FBI in January 1967 to provide a nationwide, user-oriented, computer-based, inquiry/response information system available 24 hours per day to all local, state and federal criminal justice agencies through a telecommunications network. Documented criminal justice information is stored on-line at FBI headquarters in Washington and made available upon authorized request for wanted, missing and unidentified persons; stolen and felony vehicles; stolen vehicle parts; stolen license plates; stolen and recovered guns; stolen boats; stolen securities; and other stolen articles. It

also provides an index of criminal histories and maintains information on extraditable foreign warrants. A file of individuals who have made threats against the president of the United States and other certain public officials under U.S. Secret Service protection is maintained as a locator service to that agency. Currently, the NCIC data base, which exceeds 20 million records, is queried by 59,362 authorized users who are conducting as many as one million transactions per day (an average of over 11 transactions per second). The Wanted Person File contains 335,000 subjects.

Unfortunately, the current NCIC system is unable to keep pace with the ever-increasing user demand for enhancements and new applications. Concern has also grown over NCIC's ability to meet future user requirements in a timely manner. Therefore, in January 1986, the FBI contracted for an independent, comprehensive study of NCIC requirements to serve as the foundation for the design of a new-generation NCIC to meet criminal justice needs through the year 2000.

During the study, over 485 interviews of criminal justice administrators were conducted at 180 sites throughout the 50 states, and over 200 new uses of NCIC were identified to help law enforcement efficiently carry out its mission, goals and responsibilities. One of the most requested new features was high-speed electronic image transmission of photographs, fingerprints and other pictures. A subsequent survey questionnaire sent to over 2,670 criminal justice agencies confirmed this need.

During 1989, the FBI initiated a pilot image project by combining the technology of FINGERMATRIX, Inc.,* with that of several different vendors to

develop the software and other technology configurations necessary to conduct three planned demonstrations. The demonstrations provided image transmission of a black-and-white mug shot and a fingerprint image of wanted subjects over NCIC equipment and telecommunication lines to a two-way radio base station transmitter, and out over a radio frequency into receiving equipment in a patrol car. Equipment had also been configured to permit the capture and transmission of the subject's photograph and a live-scanned fingerprint from the police car to the police station and then on to the NCIC host computer in Washington, D.C., where these images were stored in digital form on an optical disk subsystem.

The first demonstration of this image capability was given in March 1989 in the Washington, D.C., area. An FBI vehicle and two-way radio base station were used in the testing. The components that were needed in addition to the NCIC system were a centrally located optical disk unit for archival image storage interfaced to the host computer, a remote workstation comprised of a personal computer, a CCD solid-state camera for mug shot scanning and capture, a laser printer and a specialized high-resolution fingerprint scanner that scans inked fingerprints and converts them into digital images; and a transceiver device interfaced by a modem to a dedicated line to the radio base station and a synchronous link to a 56-kilobit line to the NCIC host computer.

A second demonstration of this capability was given May 1-3, 1989. The Colorado Bureau of Investigation in Denver and the Aurora, Colorado, Police Department cooperated with the FBI to transmit and receive mug shot and fingerprint images in an Aurora patrol car equipped with a mobile digital terminal. This system was connected to the Aurora radio system, then to the NCIC computer/telecommunications links to NCIC headquarters. Even though Aurora is approximately 1,480 air miles from the NCIC host computer, the uncompressed images were transmitted to the patrol car in approximately 35 seconds per frame and they were clear

and sharp in contrast. Successful tests disclosed that the patrol car does not have to be standing motionless to either send or receive good images. The car can be moving at speeds of 60 mph or more with no degradation.

The third demonstration was given at Santa Barbara, California, on May 22-24, 1989. It involved the cooperation of the California Criminal Identification and Information Branch of the California Department of Justice in Sacramento, as well as the Santa Barbara County Sheriff's Department. The image equipment was attached to a 50-watt base radio operated over an antenna mounted on top of the headquarters building and again linked to NCIC headquarters. The sheriff's department made available a patrol car with a 60-watt, push-to-talk two-way transceiver. The car was fitted with the special equipment previously described. Although Santa Barbara is approximately 2,730 miles from Washington, D.C., the resulting images were of the same high quality and could be transmitted in about the same speed as those that had been demonstrated in Aurora, Colorado.

An additional series of test involved the capture, transmission, storage, retrieval and printout of photographs and a fingerprint image of wanted fugitives for whom warrants had been issued in Santa Barbara County. The sheriff's department made available about two dozen photographs and fingerprint cards for subjects previously entered by that agency into the NCIC Wanted Persons File. The equipment was used to capture images of the photographs and the right index finger impression of these fugitives. These images were transmitted to NCIC at FBI headquarters, where they were stored on the optical disk interfaced to the NCIC host computer. Subsequent test inquiries made on these fugitives not only transmitted the text of the wanted record but also retrieved the mug shot and fingerprint image and transmitted it to the sheriff's department.

California Attorney General John K. Van DeKamp, upon attending the demonstration in Santa Barbara, commented, "The system will be even valuable in the day-to-day business of

fighting crime on the streets. Suspects who carry no ID or operate under 50 aliases in order to escape detection when stopped will be out of luck and into jail. Persons stopped for warrants issued on people with similar names or appearance will be cleared instantly, rather than taken off to jail."

The ultimate goal of NCIC 2000, relative to image transmission for the Wanted Persons File, is to assist law enforcement in the positive identification of individuals with whom the officer comes in contact. The ability to have a photograph and fingerprint transmitted within seconds to and from the patrol car provides the officer with irrefutable evidence as to whether or not an individual temporarily detained is identical to a wanted person on file at a local, state or national level. This capability will, for all practical purposes, eliminate false or erroneous arrests and could in some instances speed up the overall "stop" process.

At the present time, the FBI/NCIC staff is testing a high-speed prototype single fingerprint matcher to add to the previously tested equipment. It is expected that with this high-speed, fully automated fingerprint matcher, the Wanted Persons File could be searched within 21 seconds utilizing a single fingerprint of a potential wanted person.

The pilot image project has thus far been very successful in proving that basic building blocks of technology are available in the marketplace to support law enforcement's need for image transmission. NCIC 2000 will add this and many other new technologies to law enforcement's crime-fighting arsenal as the 21st century approaches.

Funding requests have been denied through 1991, however, and until funding is approved, the technological advances will not be realized.*

*The FBI has a long-standing policy of not endorsing any vendor's equipment except for its own use.

"Since this article was published, the 101st Congress passed legislation providing \$17 million for the building of NCIC 2000. The FBI has also been authorized to appropriate funds for Fiscal Years 1992 through 1995 to implement the NCIC 2000 project."

NCIC 2000

Many Newsletter readers participated in the NCIC 2000 Study which was conducted to identify how NCIC could be more responsive to users needs through the year 2000. NCIC users were surveyed and interviewed in 1986 as part of the Study to design a new and improved system. Users identified a significant number of concepts representing new or improved capabilities which were refined through the NCIC Advisory Policy Board and Regional Working Groups. The approved concepts include such enhancements as improved name and VIN searching techniques, access to the Canadian Police Information Center (CPIC) and to Canadian vehicle registration information, the capability to retrieve all records in the databases linked to a single crime incident or criminal, access to information about current parolees or probationers, augmentation of the size of the miscellaneous fields in records, and the creation of a new "other" category of missing persons.

A substantial number of the identified concepts addressed improvements in data quality, ease of use, system security. From these expressed user needs, the concept of a standardized NCIC workstation evolved. This workstation, when developed as part of NCIC 2000, will provide a low cost terminal with built-in help files, text editing, and security features.

A need identified by FBI managers prior to the Study was new, updated software for the NCIC host computer and telecommunications controller at FBI NCIC. The existing software dates from the inception of the System in 1967, and has far exceeded the seven-year system life cycle recommended by the National Institute for Standards and Technology (formerly National Bureau of Standards). New software will be written in a new generation language, which will improve efficiency as well as ease of maintenance.

Photograph and Fingerprint Transmission Capability

Perhaps the most important enhancement identified in the Study is the development of a more positive identification capability as part of wanted person and missing person databases. Positive identification would have two important benefits. First, positive identification would reduce or eliminate false arrests and unwarranted detention caused by hits on common names and nonunique numeric identifiers and physical descriptors. Second, the incidents of positive identifications would be increased by providing a

photograph and a fingerprint image to the officer making the inquiry. Further, the officer could, if desired, send a fingerprint image to FBI NCIC for automatic matching with prints of subjects on file to identify wanted fugitives or missing persons who attempt to use deceit or some form of false identification.

Development of these capabilities requires equipment able to store, transmit, receive, and reproduce images of fingerprints and faces for comparison with a possible wanted or missing person. The Study's goal is that this capability be usable by the patrol officer at the location of any traffic stop. Therefore, the equipment must be small enough to be accommodated comfortably in the patrol car and the images must be transmissible through two-way radio systems.

FBI NCIC, assisted by the Colorado Bureau of Investigation (CBI), the Aurora, Colorado Police Department, the Santa Barbara County, California Sheriff's Office, and the California Identification and Information Branch of the California Department of Justice has tested prototype equipment designed to make such identification capability a reality. In tests with these agencies, readable fingerprints and identifiable photographs have been electronically transmitted from a patrol car through the NCIC Network to NCIC in Washington, D.C. and have been transmitted from NCIC to a patrol car. These tests have been successfully conducted while the patrol car was stationary and also moving at speeds up to 60 m.p.h. The equipment used was easily accommodated in the patrol car, and is similar in size to some existing radio equipment. Current testing is directed towards development of a high speed fingerprint matching capability to enable the inclusion of a single fingerprint in the NCIC record which could be matched against a fingerprint of a detainee at the patrol car to ensure positive identification of wanted and missing persons.

Implementation

The NCIC Advisory Policy Board and Regional Working Groups, FBI NCIC, and the MITRE Corporation, a private systems engineering contractor, have been working to finalize implementation specifications for the NCIC 2000 enhancements, and have substantially completed this work. Certain high priority NCIC 2000 functionality which can be implemented modularly such as the CPIC interface, positive identification capability for wanted and missing persons, and improved searching techniques are planned for implementation with early funding.

(Continued on Page 6)

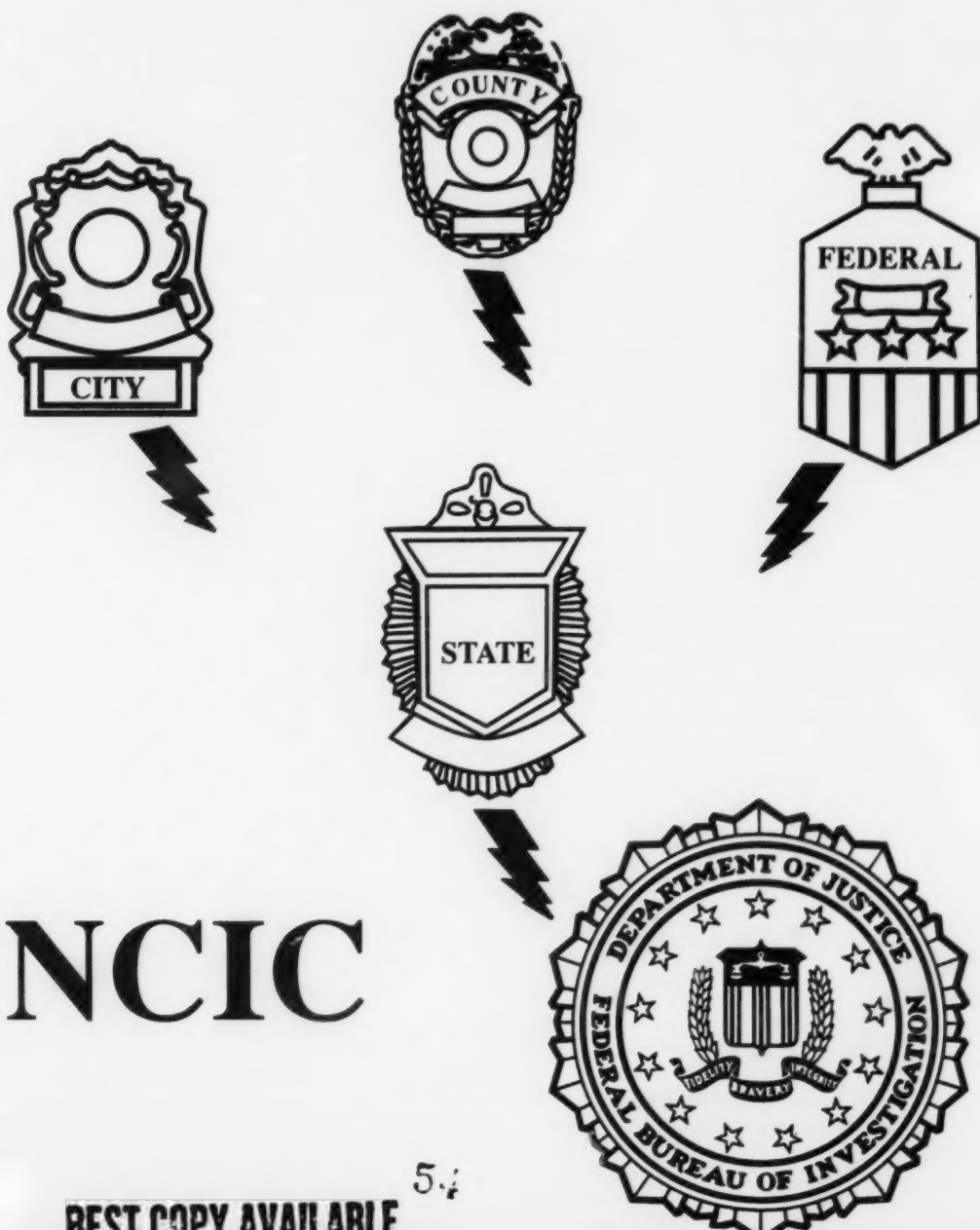
NCIC 2000 -- (Continued from page 5)

The other NCIC 2000 enhancements noted above, such as development of the workstation and new software, as well as the majority of the concepts, require specific NCIC 2000 Congress-approved funding for implementation.

The project has not been funded by Congress as yet. Prospects for funding NCIC 2000 have recently improved. Congressional authorization for the FBI for \$77 million for NCIC 2000 over five years starting in FY 1991 has been included in a

pending omnibus crime bill (S.1970). Appropriation of \$17 million has been included within H.R.5021, the House of Representatives appropriations bill which applies to the Department of Justice. This appropriation represents only first year funding. The House Appropriations Committee noted the "critical need to modernize" NCIC in its explanation of the appropriation, and the important effect of an upgraded NCIC on the war on drugs. Your state NCIC Control Terminal Agency has been working with FBI NCIC to ensure early implementation of capabilities at the state and local level once funding is available.

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: NCIC SHARED MANAGEMENT CONCEPT

TITLE OF INSTRUCTION:

NCIC Shared Management Concept

TIME ALLOTTED:

One Hour

TARGET GROUP:

Full Access Terminal Operators

INSTRUCTOR:

METHOD OF INSTRUCTION:

Lecture, Discussion,
Transparencies, and Video Tape

DATE:

July 1, 1992

7/1/92

SMC-11

**NCIC SHARED MANAGEMENT CONCEPT
TABLE OF CONTENTS**

	PAGE
STATEMENT OF GOAL AND OBJECTIVES	SMC-1
CRITERION TEST	SMC-2
CRITERION TEST ANSWERS	SMC-4
ITEMS AND MATERIALS	SMC-7
INTRODUCTION	SMC-8
DEFINITION OF THE NCIC SHARED MANAGEMENT CONCEPT	SMC-9
GOAL AND PURPOSE OF THE NCIC SHARED MANAGEMENT CONCEPT	SMC-10
NCIC ADVISORY POLICY BOARD	SMC-11
Background	SMC-11
Responsibilities	SMC-12
Accomplishments	SMC-12
NCIC REGIONAL WORKING GROUPS	SMC-14
Background	SMC-14
Responsibilities	SMC-15
NCIC USER AGREEMENT	SMC-16
Background	SMC-16
Definitions included in the NCIC User Agreement	SMC-17
FBI NCIC RESPONSIBILITIES	SMC-18
CONCLUSION	SMC-21
BIBLIOGRAPHY	SMC-22

STATEMENT OF GOAL AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator critical information on the NCIC shared management concept as it relates to NCIC and the criminal justice community.

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the terminal operator will be able to:

1. Define the NCIC shared management concept.
2. Explain the goal of the NCIC shared management concept.
3. Identify the responsibilities of the NCIC Advisory Policy Board (APB).
4. List three examples of policy mandated by the APB.
5. Identify the regions that make up the four NCIC Regional Working Groups (RWGs).
6. Define the NCIC User Agreement.
7. Define the following terms:
 - (a) State Control Terminal Agency (CTA)
 - (b) Control Terminal Officer (CTO)
 - (c) Federal Service Coordinator (FSC)
 - (d) Terminal Agency Coordinator (TAC)
8. Identify the responsibilities of the FBI under the NCIC shared management concept.

CRITERION TEST

DEFINITION SECTION

1. State the definition of the NCIC shared management concept.

GOAL AND PURPOSE SECTION

1. Explain the goal of the NCIC shared management concept.
2. State the purpose of the NCIC shared management concept.

NCIC ADVISORY POLICY BOARD (APB) SECTION

1. Identify at least three of the responsibilities of the Advisory Policy Board (APB).
2. The APB is comprised of _____ representatives from criminal justice agencies throughout the United States.

NCIC REGIONAL WORKING GROUPS (RWGs) SECTION

1. The RWGs consist of one appointed State Control Terminal Agency (CTA) representative from each state within the region and six elected local law enforcement representatives from within the region.
 - a. True
 - b. False

NCIC USER AGREEMENT SECTION

1. Define the NCIC User Agreement.
2. Define the following terms:
 - (a) Control Terminal Agency (CTA)
 - (b) Control Terminal Officer (CTO)
 - (c) Federal Service Coordinator (FSC)
 - (d) Terminal Agency Coordinator (TAC)

FEDERAL BUREAU OF INVESTIGATION (FBI) NCIC RESPONSIBILITIES SECTION

1. Identify at least two of the responsibilities of the FBI under the NCIC shared management concept.

CRITERION TEST ANSWERS

DEFINITION SECTION

1. NCIC defines the shared management concept as a cooperative Federal-state-local effort in which the FBI and authorized users share in the management and responsibility of maintaining and providing accurate and timely documented criminal justice information.

GOAL AND PURPOSE SECTION

1. The goal of the NCIC shared management concept is to ensure continued Federal, state, and local cooperation in order to arrive at workable policies and procedures to be utilized by all NCIC users.
2. The purpose of the NCIC shared management concept is to get all authorized users involved in the decision-making process.

NCIC ADVISORY POLICY BOARD (APB) SECTION

1. The responsibilities of the APB include, but are not limited to:
 - a. Recommending to the FBI general policy with respect to the philosophy, concept, and operational principles of the NCIC.
 - b. Reviewing and considering rules, regulations, and procedures for the operation of NCIC.
 - c. Considering the NCIC operational needs of criminal justice agencies in light of public policy and local, state, and Federal statutes.
 - d. Reviewing and considering security and privacy aspects of the NCIC System.

- e. Recommending standards for participation by criminal justice agencies in the NCIC System.
2. The APB is comprised of 30 representatives from criminal justice agencies throughout the United States.

NCIC REGIONAL WORKING GROUPS (RWGs) SECTION

1. True. The RWGs consist of one appointed State Control Terminal Agency representative from each state within the region and six elected local law enforcement representatives from within the region.

NCIC USER AGREEMENT

1. The NCIC User Agreement outlines the varied responsibilities of a Control Terminal Officer/Federal Service Coordinator.
2. The following terms are defined as listed below:
 - (a) CTA - a state or territorial criminal justice agency on the NCIC System providing statewide (or equivalent) service to its criminal justice users with respect to NCIC data.
 - (b) CTO - an individual appointed by the head of each CTA who will be responsible for monitoring system use, enforcing system discipline, and assuring that NCIC operating procedures are followed by all authorized users as outlined by the NCIC user agreement.
 - (c) FSC - non-CTAs with direct NCIC telecommunications lines used only for system query functions. The FSC has the same responsibilities as the CTO.
 - (d) TAC - each CTO shall ensure that each terminal agency administrator designate an individual to function as a TAC who shall be responsible for ensuring compliance with state and NCIC policy and regulations including validation* requirements.

FBI NCIC RESPONSIBILITIES SECTION

1. The responsibilities of the FBI under the NCIC shared management concept include, but are not limited to provisions of:
 - a. Operational, technical, and investigative assistance to NCIC users
 - b. Telecommunications lines to a state interface
 - c. Legal and legislative review of matters pertaining to the NCIC
 - d. Timely information on all NCIC aspects of system usage is distributed by means of the NCIC Operating Manual, NCIC Technical and Operational Updates, and related documents.
 - e. Staff Research Assistance
 - f. Training and training materials to the State Control Terminal Agencies

7/1/92

SMC-6

ITEMS AND MATERIALS

Overhead Transparencies, Projector, and Screen
VCR and Monitor
Video Tape: NCIC Responsibilities for the Agency Administrator

OVERHEAD TRANSPARENCIES (OH):

SMC-OH #1 Title Page
SMC-OH #2 Definition of the NCIC Shared Management Concept
SMC-OH #3 NCIC Advisory Policy Board
SMC-OH #4 NCIC Regional Working Groups
SMC-OH #5 NCIC User Agreement
SMC-OH #6 Definitions included in the NCIC User Agreement
SMC-OH #7 Definitions included in the NCIC User Agreement
(Continued)
SMC-OH #8 FBI NCIC Responsibilities

HANDOUTS AND MATERIALS (HD):

SMC-HD #1 NCIC Advisory Policy Board Officers and Members
SMC-HD #2 Advisory Policy Board (APB) Training Policy,
October 1984
SMC-HD #3 NCIC Regional Working Group Officers
SMC-HD #4 NCIC User Agreement
SMC-HD #5 NCIC Computerized Criminal History Program
SMC-HD #6 Bylaws for the NCIC Advisory Policy Board and
Regional Working Groups
SMC-HD #7 Control Terminal Officers and their Addresses
SMC-HD #8 Federal Agency Contacts
SMC-HD #9 NCIC Off-line Search Pamphlet
SMC-HD #10 NCIC Publications Request List
SMC-HD #11 Consideration of a Comprehensive Security Policy
Document for the NCIC System (NCIC Staff Paper)
SMC-HD #12 NCIC Training Videos

I. INTRODUCTION

THIS ONE-HOUR BLOCK OF INSTRUCTION IS DESIGNED AS A GUIDE TO AID TERMINAL OPERATORS IN BECOMING KNOWLEDGEABLE OF HOW NCIC POLICIES AND PROCEDURES ARE DEVELOPED, ENACTED, AND APPROVED.

INSTRUCTOR SHOULD WELCOME AND INTRODUCE SELF TO THE GROUP; EXPLAIN COURSE GOAL AND OBJECTIVES; REVIEW AND DISTRIBUTE HANDOUT MATERIALS.

Since January, 1967, the NCIC has operated under a shared management concept between the Federal Bureau of Investigation (FBI) and authorized users. NCIC is a computer system that interconnects elements of the Federal, state, and local criminal justice community. It represents the finest example of voluntary Federal, state, and local cooperation in the criminal justice community. Each governmental entity has independently developed a highly responsive computer network that is shared with all the members of the criminal justice community.

The forefathers of NCIC realized in 1966 that sharing of information would allow the criminal justice system to function more effectively. Charging for information would have created insurmountable costs that small states would not have been able to fund, and therefore, would not have participated in a national system.

References

OH #1

IO - INSTRUCTIONAL
OBJECTIVE

OH - OVERHEAD
TRANSPARENCY

HD - HANDOUT
MATERIAL

7/1/92

SMC-8

II. DEFINITION OF THE NCIC SHARED MANAGEMENT CONCEPT

IO #1

OH #2

NCIC defines the shared management concept as a cooperative **Federal-state-local** effort in which the Federal Bureau of Investigation (FBI) and authorized users share in the management and responsibility of maintaining and providing **accurate and timely** documented criminal justice information.

7/1/92

SMC-9

III. GOAL AND PURPOSE OF THE NCIC SHARED MANAGEMENT
CONCEPT

IO #2

A. Goal

1. The goal of the NCIC shared management concept is to ensure continued Federal, state, and local cooperation in order to arrive at workable policies and procedures to be utilized by all NCIC users.

B. Purpose

1. The purpose of the NCIC shared management concept is to get all authorized users involved in the decision-making process.

IV. NCIC ADVISORY POLICY BOARD (APB)

OH #3

A. Background

1. The APB was established in February, 1969, by the Director, FBI to aid in the development of NCIC. The Board is comprised of 30 representatives from criminal justice agencies throughout the United States.
 - a. Twenty members are elected for two-year terms. Since NCIC is divided into four regions, i.e., North Central, Northeastern, Southern, and Western, five are from each of the four NCIC regions.

HD #1

INSTRUCTOR'S NOTE: REFER TO SECTION V OF THIS LESSON PLAN: NCIC REGIONAL WORKING GROUPS.

- b. Six members are appointed by the Director of the FBI for an indefinite term. Two of the six appointees represent the judiciary; two represent prosecutory agencies; and the remaining two represent correctional agencies.
 - c. The four additional members are representatives from the:
 - (1) International Association of Chiefs of Police
 - (2) National Sheriff's Association
 - (3) National District Attorneys' Conference
 - (4) National Probation and Parole Association
 - d. The Chairman of the Board must be one of the 20 elected members and the Board must meet at least twice a year.

B. Responsibilities

IO #3

Responsibilities of the APB include, but are not limited to:

1. Recommending to the FBI general policy with respect to the **philosophy, concept, and operational principles** of the NCIC.
2. Reviewing and considering rules, regulations, and procedures for the operation of NCIC.
3. Considering the NCIC operational needs of criminal justice agencies in light of public policy and local, state, and Federal statutes.
4. Reviewing and considering security and privacy aspects of the NCIC System.
5. Recommending standards for participation by criminal justice agencies in the NCIC System.

C. Accomplishments

IO #4

1. At the December, 1990, meeting the APB recommended that the Bureau of Alcohol, Tobacco and Firearms (ATF) Violent Felon File be implemented to identify violent felony offenders.
2. In October, 1984, in response to the NCIC Audit Staff's findings, the APB established a mandatory training program.
 - a. The APB ordered that by 12/31/86 each State Control Terminal Agency establish a training program which would not be limited to but include entry-level training and in-service training on NCIC use.

INSTRUCTOR'S NOTE: PLEASE REFER TO THE HANDOUT ON THE NCIC TRAINING POLICY AS APPROVED BY THE APB (OCTOBER, 1984). THE APB LATER APPROVED THE REFORMULATION OF THE NCIC TRAINING POLICY AND NCIC ADVISED ALL CTOs AND FSCs BY MEMORANDUM DATED 9/11/91.

HD #2

3. In December, 1978, the APB approved a policy which allows one agency to act as holder of the record for another agency provided an agreement is signed between the two agencies.

7/1/92

SMC-13

V. NCIC REGIONAL WORKING GROUPS (RWGs)

A. Background

1. The RWGs were established to implement policy and procedures established for the National Crime Information Center. Four RWGs were established throughout the United States. The RWGs are:
 - a. **North Central** - Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, Wisconsin
 - b. **Northeastern** - Canada, Connecticut, Delaware, District of Columbia, Federal agencies, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont
 - c. **Southern** - Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, Commonwealth of Puerto Rico, South Carolina, Tennessee, U.S. Virgin Islands, Virginia, West Virginia
 - d. **Western** - Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Texas, Utah, Washington, Wyoming
2. The RWGs consist of **one** appointed State Control Terminal Agency representative from each state within the region and **six** elected local law enforcement representatives from within the region.
3. Each region has a Chairman, First Vice Chairman and Second Vice-Chairman.
4. The RWGs meet from time to time to consider NCIC policy and operational issues. These meetings will constitute a regional meeting to inform NCIC participants of the current status of the NCIC program and seek users views on various NCIC issues.

OH #4

IO #5

HD #3

B. Responsibilities

1. Reviewing operational issues of the NCIC System
and
2. Making appropriate recommendations to the NCIC Advisory Policy Board.
 - a. The ideas and concepts recommended for enhancement of the NCIC System are initiated by the users. If an NCIC user has a suggestion, the suggestion should be submitted through the following chain:
 - (1) Terminal Operator
 - (2) Terminal Agency Coordinator
 - (3) Control Terminal Officer/
Service Coordinator
 - (4) National Crime Information Center
 - (5) Regional Working Groups
Committee
 - (6) Advisory Policy Board
 - (7) Director, FBI

**INSTRUCTOR'S NOTE: EMPHASIZE TO THE
TERMINAL OPERATOR(S) THAT THIS IS A
COOPERATIVE VENTURE AND ALL SUGGESTIONS CAN
BE CONSIDERED WHEN USING APPROPRIATE LINES
OF COMMUNICATION.**

VI. NCIC USER AGREEMENT

IO #6
HD #4

A. Background

1. The NCIC User Agreement outlines the varied responsibilities of a Control Terminal Officer/Federal Service Coordinator (CTO/FSC). The documents listed below are incorporated by reference and made a part of the user agreement.

OH #5

- a. NCIC Operating Manual
- b. NCIC Computerized Criminal History (CCH) Program Background, Concept and Policy as amended or superseded by implementation of the Interstate Identification Index (III) Program.

HD #5

INSTRUCTOR'S NOTE: REFER TO THE NCIC INTERSTATE IDENTIFICATION INDEX LESSON PLAN FOR MORE INFORMATION.

- c. Minutes of the NCIC Advisory Policy Board
- d. ByLaws for the NCIC APB and RWGs
- e. Title 28, Code of Federal Regulations, Part 20
- f. NCIC Standards as recommended by the NCIC APB and approved by the FBI, Director.

HD #6

INSTRUCTOR'S NOTE: REFER TO THE NCIC STANDARDS AND SANCTIONS LESSON PLAN FOR MORE INFORMATION.

- g. Applicable Federal and state law and regulation.
2. The APB (March 1984) mandated that each state group sign a user agreement with NCIC.
3. The NCIC APB established a goal of having a single state agency in each state assume responsibility as the NCIC

Control Terminal Agency (CTA) for the state, through and by which NCIC users in that state would access NCIC.

4. The Board approved the CTA concept in order to unify responsibility for system user discipline and adherence to system procedures and policies within each state. The CTA also serves as a central point of contact in its state for handling record validations, quality control matters, dissemination of manuals and other NCIC publications, security matters, user training, audit, and any other problems concerning system use.

B. Definitions included in the NCIC User Agreement

OH #6, 7

1. **CTA** - a state or territorial criminal justice agency on the NCIC System providing statewide (or equivalent) service to its criminal justice users with respect to NCIC data.
2. **CTO** - an individual appointed by the head of each CTA who will be responsible for monitoring system use, enforcing system discipline, and assuring that NCIC operating procedures are followed by all authorized users as outlined by the NCIC user agreement.
3. **FSC** - Non-CTAs with direct NCIC telecommunications lines used only for system query functions. The FSC has the same responsibilities as the CTO.
4. **TAC** - each CTO shall ensure that each terminal agency administrator designate an individual to function as a **TAC** who shall be responsible for ensuring compliance with state and NCIC policy and regulations including validation* requirements.

IO #7

HD #7

HD #8

***INSTRUCTOR'S NOTE: PLEASE REFER TO THE VALIDATION LESSON PLAN FOR MORE INFORMATION.**

VII. FEDERAL BUREAU OF INVESTIGATION (FBI) NCIC RESPONSIBILITIES

IO #8

- A. The FBI NCIC responsibilities under the shared management concept include, but are not limited to provisions of:

OH #8

1. **Operational, technical, and investigative** assistance to NCIC users. Examples include, but are not limited to:

- a. The **Investigative Off-line Search** - a special query of the NCIC System for information not obtainable on line.
- b. Assisting users in answering technical and operational questions.

HD #9

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA AND REGIONAL INTERFACE (IF APPLICABLE) AS MANY STATE AND INTERFACE SYSTEMS MAY HAVE DIFFERENT SEARCH CRITERIA OR CONTACT THE NCIC INVESTIGATIVE SUPPORT GROUP, FBI NCIC (202) 324-6242 OR ORI/DCFBIWAT8, FOR MORE INFORMATION.

- c. The **Delayed Inquiry (Q)** - a search of the NCIC Vehicle, Wanted Person, and Missing Person Files for inquiries made 72 hours prior to entry.

INSTRUCTOR'S NOTE: CONTACT THE NCIC COMMUNICATION INFORMATION ANALYST GROUP, (202) 324-5134 OR ORI/DCFBIWAQ9, FOR MORE INFORMATION.

2. Telecommunications lines to a state interface
 - a. Telecommunications lines extend from NCIC to the state CTA and from the CTA to its users. The telecommunications lines from the FBI to the CTA is subsidized by the FBI. The cost of the telecommunications lines from the CTA to its users is the responsibility of the CTA.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CONTROL TERMINAL AGENCY AND REGIONAL INTERFACE (IF APPLICABLE) FOR INFORMATION ON THE COST OF TELECOMMUNICATIONS LINES TO LOCAL AUTHORIZED USERS.

3. Legal and legislative review of matters pertaining to the NCIC

- a. Responsible for legal and legislative review of information, e.g., The National Child Assistance Act of 1990 mandated that each Federal, state, and local law enforcement agency report each case of a missing child under the age of 18 to the NCIC of the Department of Justice.

4. Timely information on all NCIC aspects of system usage is distributed by means of the NCIC Operating Manual, NCIC Technical and Operational Updates, and related documents. FBI NCIC provides the following NCIC materials/publications:

HD #10

- a. NCIC Operating Manual
- b. NCIC Code Manual
- c. NCIC Technical and Operational Update
- d. NCIC Newsletter
- e. Other related documents, e.g., NCIC File Reference Card

INSTRUCTOR'S NOTES: PLEASE REFER TO THE FBI NCIC PUBLICATIONS REQUEST LIST.

EMPHASIZE TO THE TERMINAL OPERATOR(S) THAT THE FBI NCIC DISTRIBUTE NCIC MATERIALS TO THE CTA/FSC AND IT IS THE RESPONSIBILITY OF THE CTA/FSC TO DISTRIBUTE TO ALL USERS UNDER THEIR SERVICE JURISDICTION.

5. Staff Research Assistance

- a. The NCIC Research Staff provides assistance regarding policy matters

HD #11

before the APB, e.g., a Staff paper entitled: **"Consideration of Comprehensive Security Policy Document for the NCIC System"** - all current policy dealing with security in effect.

6. Training and training materials to the Control Terminal Agencies

- a. To develop a **Mandatory Minimum Standards Curriculum for Full Access Terminal Operators** by providing lesson plans, e.g., Ad Hoc Training Subcommittee.
- b. **NCIC Training Videos/Facilitator Guides** - FBI NCIC produces training videos and facilitator guides to be used by NCIC users throughout the criminal justice system. These videos and guides provide training by presenting relevant information concerning important justice issues such as missing children, wanted persons, unidentified persons, and stolen property, as well as the development of an updated crime information computer system, NCIC 2000.

HD #12

INSTRUCTOR'S NOTE: PLEASE REFER TO THE CURRENT LIST OF TRAINING VIDEOS AVAILABLE. FOR ADDITIONAL INFORMATION ON NCIC TRAINING VIDEOS, PLEASE CONTACT THE NCIC VIDEO TRAINING STAFF, (202) 324-2011.

VIII. CONCLUSION

NCIC continues to operate as a cooperative Federal-state-local venture, with policy recommended by the APB and set by the FBI on the basis of input by authorized users.

It is important to remember:

1. The **NCIC shared management concept** is a cooperative Federal-state-local effort in which the FBI and authorized users share in the management and responsibility of maintaining and providing accurate and timely documented criminal justice information.
2. The **NCIC Advisory Policy Board** makes recommendations to the Director of the FBI with respect to the philosophy, concept, and operational principles of the NCIC.
3. The **NCIC Regional Working Groups** were established to implement policy and procedures established for the NCIC.
4. The **NCIC User Agreement** outlines the varied responsibilities of the CTO/FSC.
5. The **FBI provides technical, operational, and investigative assistance** to NCIC users.

When used correctly, NCIC and state systems are valuable tools to assist the criminal justice community. Accomplishing its goal requires unparalleled cooperation between Federal, state, and local criminal justice agencies.

INSTRUCTOR'S NOTE: SHOW "NCIC RESPONSIBILITIES FOR THE AGENCY ADMINISTRATOR" VIDEO (VIDEO PLAYING TIME - 12:56 MINUTES.)

BIBLIOGRAPHY

- Federal Bureau of Investigation. National Crime Information Center. Washington, DC. National Crime Information Center: A Newsletter for the Criminal Justice Community. Volume 24, No. 2. August, 1991.
- Federal Bureau of Investigation. National Crime Information Center. Washington, DC. National Crime Information Center: A Newsletter for the Criminal Justice Community. Volume 24, No. 1. April, 1991.
- Federal Bureau of Investigation. National Crime Information Center. Washington, DC. NCIC Newsletter. 88-1. "The NCIC Advisory Policy Board." p. 3.
- Federal Bureau of Investigation. National Crime Information Center. Washington, DC. NCIC Newsletter. Fall, 1985. "The NCIC Advisory Policy Board." p. 1.
- Federal Bureau of Investigation. National Crime Information Center. Washington, DC. NCIC Operating Manual. May 31, 1989. Revision 55.
- Federal Bureau of Investigation. National Crime Information Center. "NCIC Responsibilities for the Agency Administrator" Video. June, 1990. 12:56 Minutes.
- Federal Bureau of Investigation. National Crime Information. Washington, DC. NCIC Technical and Operational Update. 91-4. "Implementation of the Bureau of Alcohol, Tobacco, and Firearms (ATF) Violent Felon File" p. 2-1.
- U.S. Department of Justice. Federal Bureau of Investigation. Washington, DC. National Crime Information Center - The Investigative Tool: A guide to the use and Benefits of NCIC. June, 1986.
- U.S. Department of Justice. Federal Bureau of Investigation. Washington, DC. National Crime Information Center. Bylaws for the NCIC Advisory Policy Board and Regional Working Groups. October 17, 1984.

OVERHEAD TRANSPARENCIES (OH)

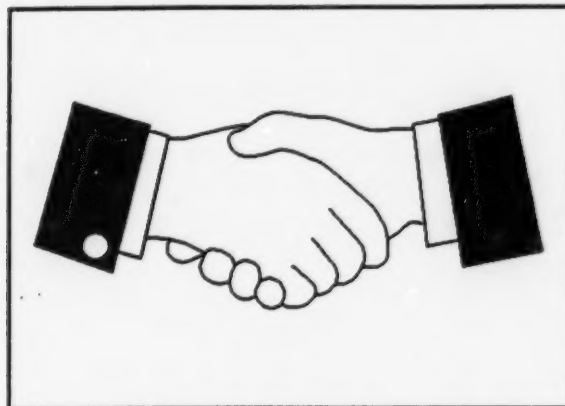
NATIONAL CRIME INFORMATION CENTER

NCIC SHARED MANAGEMENT CONCEPT

7/1/92

SMC-OH #1

**DEFINITION OF THE
NCIC SHARED MANAGEMENT CONCEPT**



**NCIC DEFINES THE SHARED MANAGEMENT CONCEPT AS A
COOPERATIVE FEDERAL-STATE-LOCAL EFFORT IN WHICH THE FBI
AND AUTHORIZED USERS SHARE IN THE MANAGEMENT AND
RESPONSIBILITY OF MAINTAINING ACCURATE AND TIMELY
DOCUMENTED CRIMINAL JUSTICE INFORMATION.**

• nonvoting members



NCIC REGIONAL WORKING GROUPS

NORTH CENTRAL

**ILLINOIS, INDIANA, IOWA, KANSAS,
MICHIGAN, MINNESOTA, MISSOURI,
NEBRASKA, NORTH DAKOTA, OHIO,
SOUTH DAKOTA, WISCONSIN**

NORTHEASTERN

**CANADA, CONNECTICUT, DELAWARE,
DISTRICT OF COLUMBIA, FEDERAL
AGENCIES, MAINE, MARYLAND,
MASSACHUSETTS, NEW HAMPSHIRE,
NEW JERSEY, NEW YORK,
PENNSYLVANIA, RHODE ISLAND,
VERMONT**

SOUTHERN

**ALABAMA, ARKANSAS, FLORIDA,
GEORGIA, KENTUCKY, LOUISIANA,
MISSISSIPPI, NORTH CAROLINA,
OKLAHOMA, COMMONWEALTH OF
PUERTO RICO, SOUTH CAROLINA,
TENNESSEE, U.S. VIRGIN ISLANDS,
VIRGINIA, WEST VIRGINIA**

WESTERN

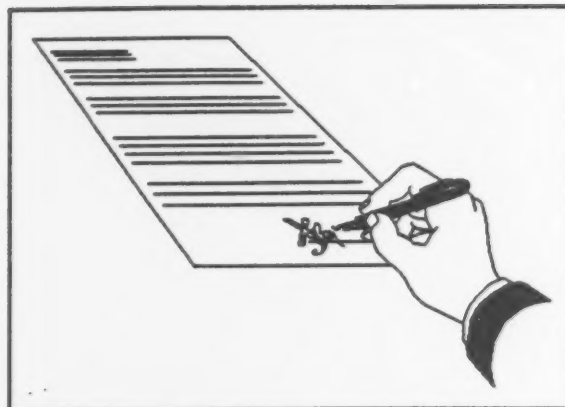
**ALASKA, ARIZONA, CALIFORNIA,
COLORADO, HAWAII, IDAHO,
MONTANA, NEVADA, NEW MEXICO,
OREGON, TEXAS, UTAH,
WASHINGTON, WYOMING**

7/1/92

SMC-OH #4

NCIC USER AGREEMENT

THE FOLLOWING DOCUMENTS
LISTED BELOW ARE
INCORPORATED BY
REFERENCE AND MADE A PART
OF THE NCIC USER
AGREEMENT:



*

NCIC OPERATING MANUAL

*

NCIC COMPUTERIZED CRIMINAL HISTORY (CCH)
PROGRAM BACKGROUND, CONCEPT AND POLICY AS
AMENDED OR SUPERSEDED BY IMPLEMENTATION OF
THE INTERSTATE IDENTIFICATION INDEX (III) PROGRAM

*

MINUTES OF THE NCIC APB

*

BY LAWS FOR THE NCIC APB AND RWGs

*

TITLE 28, CODE OF FEDERAL REGULATIONS, PART 20

*

NCIC STANDARDS AS RECOMMENDED BY THE NCIC APB
AND APPROVED BY THE FBI, DIRECTOR

*

APPLICABLE FEDERAL AND STATE LAW AND
REGULATION

DEFINITIONS INCLUDED IN THE NCIC USER AGREEMENT

CONTROL TERMINAL AGENCY (CTA):

A STATE OR TERRITORIAL CRIMINAL JUSTICE AGENCY ON THE NCIC SYSTEM PROVIDING STATEWIDE (OR EQUIVALENT) SERVICE TO ITS CRIMINAL JUSTICE USERS WITH RESPECT TO NCIC DATA.

CONTROL TERMINAL OFFICER (CTO):

AN INDIVIDUAL APPOINTED BY THE HEAD OF THE CTA WHO WILL BE RESPONSIBLE FOR MONITORING SYSTEM USE, ENFORCING SYSTEM DISCIPLINE, AND ASSURING THAT NCIC OPERATING PROCEDURES ARE FOLLOWED BY ALL AUTHORIZED USERS AS OUTLINED BY THE NCIC USER AGREEMENT.

**DEFINITIONS INCLUDED IN THE NCIC USER AGREEMENT
(CONTINUED)**

FEDERAL SERVICE COORDINATOR (FSC):

NONCONTROL TERMINAL AGENCIES WITH DIRECT NCIC TELECOMMUNICATIONS LINES USED ONLY FOR SYSTEM QUERY FUNCTIONS. THE FSC HAS THE SAME RESPONSIBILITIES AS THE CTO.

TERMINAL AGENCY COORDINATOR (TAC):

EACH CONTROL TERMINAL OFFICER SHALL ENSURE THAT EACH TERMINAL AGENCY ADMINISTRATOR DESIGNATE AN INDIVIDUAL TO FUNCTION AS A TAC WHO SHALL BE RESPONSIBLE FOR ENSURING COMPLIANCE WITH STATE AND NCIC POLICY AND REGULATIONS INCLUDING VALIDATION REQUIREMENTS.

FBI NCIC RESPONSIBILITIES



INCLUDE, BUT ARE NOT LIMITED TO PROVISIONS OF:

- 1. OPERATIONAL, TECHNICAL, AND INVESTIGATIVE ASSISTANCE TO NCIC USERS**
- 2. TELECOMMUNICATIONS LINES TO A STATE INTERFACE**
- 3. LEGAL AND LEGISLATIVE REVIEW OF MATTERS PERTAINING TO NCIC**
- 4. TIMELY INFORMATION ON ALL NCIC ASPECTS OF SYSTEM USAGE IS DISTRIBUTED BY MEANS OF THE NCIC OPERATING MANUAL, NCIC TECHNICAL AND OPERATIONAL UPDATES, AND RELATED DOCUMENTS**
- 5. STAFF RESEARCH ASSISTANCE**
- 6. TRAINING AND TRAINING MATERIALS TO THE CTAs**

HANDOUT MATERIALS (HD)

NCIC ADVISORY POLICY BOARD

OFFICERS

Chairman

Mr. Patrick J. Doyle
Director
Division of Criminal Justice
Information Systems
Florida Department of Law Enforcement
Post Office Box 1489
Tallahassee, FL 32302

904-488-3961
FAX 904-487-1030

First Vice Chairman

Mr. Thomas J. Nestel
Deputy Police Commissioner
Police Administration Building
Franklin Square, Room 312
Philadelphia, PA 19106

215-592-5878
FAX 215-625-0307

Second Vice Chairman

Mr. W. Gray Buckley
Inspector
Colorado Bureau of Investigation
Suite 3000
690 Kipling Street
Denver, CO 80215

303-239-4224 or 4222
FAX 303-235-0568

5/13/92

MEMBERS

North Central Region

Mr. Kenneth A. Bentfield, Director
Office of Information Systems Management
Minnesota Department of Public Safety
Room 314, Transportation Building
395 John Ireland Blvd.
St. Paul, MN 55155

612-296-7589
FAX 612-297-5728

Mr. David R. Ferguson
Director, Criminal Justice Data Center
Michigan Department of State Police
714 South Harrison Road
East Lansing, MI 48823

517-336-6555
FAX 517-336-6256

Mr. Gene P. Marlin
Deputy Director
Illinois State Police
103 Armory Building
P. O. 19461
Springfield, IL 62794-9461

217-782-7263
FAX 217-785-2821

Major William H. Trimble
Kansas City Police Department
1125 Locust Street
Kansas City, MO 64106

816-353-3974
FAX 816-234-5013

Major David L. Hornbaker
Kansas Highway Patrol
122 Southwest Seventh Street
Topeka, KS 66603

913-296-6800
FAX 913-296-5956

5/13/92

Northeastern Region

Major James R. Amos
Director
Bureau of Technical Services
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110

717-783-5588
FAX 717-783-4384

Colonel Clifford M. Gravier
Superintendent
Delaware State Police
Post Office Box 430
Dover, DE 19903

302-739-5911
FAX 302-739-5966

Lt. Col. Richard Jankowski
New Jersey State Police
Post Office Box 7068
West Trenton, NJ 08628-0068

609-882-2000
Ext. 2211
FAX 609-882-6920

Mr. Thomas J. Nestel
Deputy Police Commissioner
Police Administration Building
Franklin Square, Room 313
Philadelphia, PA 19106

215-592-5878 or 5877
FAX 215-592-5637

Lt. Colonel Robert Horton
Director
Vermont State Police
103 S. Main Street
Waterbury, VT 05676

802-244-7345
FAX 802-244-1106

5/13/92

Southern Region

Mr. Louie C. Caudell
Chief of Police
Little Rock Police Department
700 West Markham Street
Little Rock, AR 72201

501-371-4621
FAX 501-371-4892

Mr. William C. Corley
Assistant Director
Division of Criminal Information
State Bureau of Investigation
407 North Blount Street
Raleigh, NC 27601-1009

919-733-3171
FAX 919-733-8378

Mr. Patrick J. Doyle
Director
Division of Criminal Justice
Information Systems
Florida Department of Law Enforcement
Post Office Box 1489
Tallahassee, FL 32302

904-488-3961
FAX 904-487-1030

Captain James V. Martin
South Carolina Law Enforcement Division
Post Office Box 21398
Columbia, SC 29221

803-737-9029
FAX 803-737-3796

Mr. Thomas J. McGreevy
Deputy Director
Georgia Crime Information Center
Georgia Bureau of Investigation
Post Office Box 370748
Decatur, GA 30037-0748

404-244-2601
FAX 404-241-5992

5/13/92

Western Region

Mr. Joseph P. Bonino
Commanding Officer
Records and Identification Division
Los Angeles Police Department
150 North Los Angeles Street, Room 210
Los Angeles, CA 90012

213-485-2601
FAX 213-237-0380

Mr. W. Gray Buckley
Inspector
Colorado Bureau of Investigation
690 Kipling Street, Suite 3000
Denver, CO 80215

303-239-4224 or 4222
FAX 303-235-0568

Mr. A. D. Jones
Chief
Criminal Identification Bureau
Idaho Department of Law Enforcement
6064 Corporal Lane
Boise, ID 83704

208-327-7137
FAX 208-327-7138

Mr. Richard J. Townsend
Director
Bureau of Criminal Identification
Department of Public Safety
4501 South 2700 West
Salt Lake City, UT 84119

801-965-4395
FAX 801-965-4749

Mr. Fred H. Wynbrandt
Chief
Bureau of Criminal Identification and Analysis
California Department of Justice
Post Office Box 903387
Sacramento, CA 94203-3870

916-739-3936
FAX 916-739-5495

5/13/92

Criminal Justice Community Representatives

Honorable Deborah J. Daniels
United States Attorney
Southern District of Indiana
U.S. Courthouse, 5th Floor
46 East Ohio Street
Indianapolis, IN 46204

317-226-6333
FAX 317-226-6125
or FTS 331-6125

Honorable William H. Fauver
Commissioner
New Jersey State Department of Corrections
CN 863
Trenton, NJ 08625-0863

609-292-9860 or 4036
FAX 609-777-0445

Mr. Wade B. Houk
Assistant Director, Administration
Federal Bureau of Prisons
Room 454
320 First Street, Northwest
Washington, DC 20534

202-307-3230
FAX 202-514-6878
or FTS 367-3230

Honorable Manuel L. Real
Chief Judge
United States District Court
Central District of California
312 North Spring Street
Los Angeles, CA 90012

213-894-5267
FTS 798-5267
FAX 213-894-3389

5/13/92

Criminal Justice Professional Association Representatives

American Probation and Parole Association

Mr. Harvey M. Goldstein
Assistant Director for Probation
Administrative Office of the Courts
CN 987
Trenton, NJ 08625

609-292-1589
FAX 609-984-3630

National Sheriffs' Association

Mr. Charles Meeks
Executive Director
National Sheriffs' Association
1450 Duke Street
Alexandria, VA 22314

703-836-7827
FAX 703-683-6541

National District Attorneys Association

Honorable Sandra A. O'Connor
State's Attorney
Baltimore County
County Courts Building
401 Bosley Avenue
Towson, MD 21204

301-887-6600
FAX 301-887-6646

International Association of Chiefs of Police

Mr. David G. Walchak
Chief of Police
Concord Police Department
35 Green Street
Concord, NH 03301-4299

603-225-8600
FAX 603-228-2703

5/13/92



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

September 11, 1991

TO: ALL CONTROL TERMINAL OFFICERS (CTOs) AND FEDERAL SERVICE
COORDINATORS

THIS LETTER, AND THE ATTACHED DOCUMENTATION, MAY
REQUIRE SIGNIFICANT CHANGES TO YOUR NATIONAL CRIME INFORMATION
CENTER (NCIC) TRAINING PROGRAM.

During the December, 1989 meeting of the Advisory Policy Board, the Chairman appointed a Training Ad Hoc Subcommittee to address a number of key training issues that affect all Control Terminal Agencies (CTAs). This letter contains a succinct summary of the deliberations of the Training Ad Hoc Subcommittee and the Advisory Policy Board, and highlights changes in policy.

The Advisory Policy Board has approved a significant reformulation of NCIC training policy as follows (underlining identifies parts of the policy that have been changed):

"(1) Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

"(2) Biennially, provide functional retesting, and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

"(3) Maintain records of all training, testing, and proficiency affirmation.

"(4) Initially (within 12 months of employment or assignment) all sworn law enforcement personnel must receive basic training in NCIC matters to ensure effective use of the System and compliance with NCIC policy and regulation."

"(5) Make available appropriate training on NCIC System use for criminal justice practitioners other than sworn personnel."

"(6) All sworn law enforcement personnel and other practitioners should be provided with continuing access to information concerning NCIC/state systems, using methods such as roll call and in-service training."

"(7) Provide peer level training on NCIC System use, regulations, policy, audits, sanctions, and related civil liability for criminal justice administrators and upper level managers."

"(8) Annually review all curricula for relevancy and effectiveness."

Item number two has been changed in response to a suggestion from a CTO. The CTO noted that the requirement to retrain all terminal operators every two years was a duplicative burden since most terminal operators receive continual, informal, on-the-job training. The initial proposal was to extend the retraining period to three years; however, after much discussion, the Training Subcommittee determined that modification of the policy to require functional retesting and reaffirmation of proficiency every two years would address the problem. By implication, if a terminal operator fails the functional retesting, the operator must be retrained. The Subcommittee also discussed the issue of functional retesting, and noted that the CTO is the proper individual to define functional retesting on the state system. Functional retesting may be administered with or without the use of a terminal.

The requirement to maintain records of all training, testing, and proficiency affirmation remains. It is now number three in the requirements. This is a significant change since it is the intent of the Training Subcommittee and the Advisory Policy Board to limit the duty to maintain individual training records to terminal operators. The CTA still has a duty to ensure that records are kept concerning the training of other individuals using the system, but these records need not be maintained on an individual basis. For example, the CTO must

ensure that an individual record is kept concerning the training and retraining of each dispatcher using NCIC. The record may be kept by the CTA or, if the CTO chooses to decentralize training, by the local agency. Records must be kept concerning training of other individuals, such as sworn officers, but the records need not be kept on an individual basis. For example, if rookie sworn personnel receive training in NCIC matters during their basic school, this fact should be documented by the CTA. It is not necessary maintain documentation concerning each individual officer.

Item four sets a higher standard of training for sworn law enforcement personnel than for other members of the criminal justice community. Item four requires that all sworn personnel must receive basic training. Essentially, sworn personnel must receive formal training during the first 12 months on the job.

Item five addresses other practitioners such as district attorney's, judges, etc.. These individuals must have training made available to them. The CTO may address this requirement by appearing at professional seminars, providing videos, or any other method that will familiarize other practitioners with NCIC and the state system.

Item six eliminates the previous requirement to retrain all sworn personnel and other practitioners every two years. The need to provide continual training has been substituted for the biennial requirement. This may be done through roll-call or similar methods.

In order to address continuing questions, definitions of "full service" and "less than full service" terminal operators were developed. A "full access" or "full service" operator is a terminal operator who may be called upon to perform all NCIC functions. An operator is a "full access" operator if the duties, whether full-time, part-time, or occasional, require the capability to perform the full range of NCIC functions. Any individual, whether sworn or nonsworn, who is a "full access" operator must attend a training program that includes all items specified in the mandatory minimum standards curriculum for terminal operators set forth in this letter.

The "less than full access" operator is any individual who has occasion to use a terminal but who is not required to perform all NCIC functions. A "less than full access" operator must have training that is appropriate to the level of access permitted, a degree of training that may be less than that required for the "full access" operator. A full discussion of the "full access" versus "less than full access" operator is

included in the attached staff paper entitled "Reformulation of the NCIC Training Curriculum."

The second significant change established A MANDATORY MINIMUM CURRICULUM FOR "FULL-SERVICE" TERMINAL OPERATORS. All state training programs must include each of the following items in their training curriculum for full service operators:

I. SYSTEM HISTORY

- A. Description of NCIC - organizational authority
- B. Purpose of the System
- C. Authorized User Agencies
- D. Available Files

II. SHARED MANAGEMENT CONCEPT

- A. Goal
- B. Purpose
- C. Advisory Policy Board
- D. Regional Working Groups

III. INTERRELATIONSHIP OF STATE AND NCIC SYSTEM (IF APPLICABLE)

- A. Duplicate Entries
- B. Different Criteria

IV. NCIC AND STATE FILES

- A. Available Files
- B. Criteria
- C. Inquiry, Entry, Modify, Clear, Cancel & Locate Capabilities
- D. Cross Search (\$M, \$N)
- E. Interpreting Responses
- F. Specialized Searches

V. HIT CONFIRMATION

- A. Definition of a Hit
- B. Probable Cause
- C. Ten-minute Hit Confirmation Policy
- D. Confirming a Hit

VI. SYSTEM SECURITY

- A. Physical Security of Terminal and Printouts
- B. Confidentiality
- C. Access Eligibility
- D. Dissemination

VII. INTERSTATE IDENTIFICATION INDEX

- A. Description
- B. How to Use/Criteria for Entry
- C. Permissible Uses
- D. Manual Files
- E. Logging Requirements/Use of Attention Field
- F. Privacy/Security Interests
- G. Purpose Codes
- H. Primary/Secondary Dissemination
- I. Liability

VIII. QUALITY CONTROL

- A. Responsibilities
 - 1. Federal and State
 - a. Automatic Computer Edits
 - b. Automatic Purging of Records

- c. Quality Control (e.g. Serious and Form Errors, Trends and Administrative Messages)
 - d. Validations
- 2. Entering Agencies - Record Quality
 - a. Timeliness
 - b. Accuracy
 - c. Completeness/Packing the Record - Sources

IX. VALIDATION REQUIREMENT

- A. Definition
- B. Local Agency Procedures for Validating as it Relates to the Terminal Operator
- C. Penalties for Failure to Validate Records

X. STANDARDS AND SANCTIONS

- A. State and Federal Audits
- B. Sanctions Program
- C. Testing and Proficiency Affirmation

XI. LIABILITY

- A. III
- B. Hit Confirmation
- C. Data Quality/Validation

XII. DOCUMENTATION

- A. Entries
- B. Hits
- C. Validations

The NCIC Training Staff is preparing a lesson plan for each of the twelve sections set out in the mandatory minimum curriculum. USE OF THESE LESSON PLANS WILL BE OPTIONAL; however,

each item in the minimum curriculum must be addressed in the state program.

The third change involved creation of a RECOMMENDED MINIMUM TRAINING REQUIREMENT for sworn personnel. This is a suggested curriculum, not mandatory.

- I. FILES
 - A. Provide a Working Knowledge of All NCIC/State Files (Including Criteria for Entry, Complete Utilization of Fields, Importance of III, etc.)
- II. PACKING THE RECORD
 - A. Familiarization with Available Resources to Place Complete and Accurate Information into the System
- III. DISSEMINATION
 - A. Restrictions on Use of NCIC Data (Including III)
- IV. DOCUMENTATION
 - A. Proper Record Keeping
 - 1. Case File
 - 2. 2nd Party Check
- V. HIT CONFIRMATION
 - A. 10-Minute Policy
 - B. Probable Cause
 - C. Extradition Matters
- VI. INVESTIGATIVE ASSISTANCE
 - A. Specialized Searches
 - 1. State Capabilities
 - 2. Federal Capabilities
- VII. LIABILITY
 - A. Data Quality
 - B. Validation

A full discussion of the issue of "who is a practitioner" and the degree of training required is included in the attached staff paper.

The issue of "certification" versus "affirmation of proficiency" was discussed by the Subcommittee in detail. The Subcommittee reemphasized the fact that the Advisory Policy Board rejected certification as an NCIC requirement in favor of the term "affirmation of proficiency." States have wide latitude in developing the method used to affirm proficiency. The CTO may require certification as part of state policy.

The attached staff paper includes a discussion and rationale of the changes in the NCIC training policy. It addresses many frequently asked training questions, and attempts to erase misunderstandings that have developed since implementation of the training policy in 1984.

For your information, the NCIC Audit Staff is currently amending the audit protocol to include the mandatory minimum curriculum as a part of the audit review. The Audit Staff will use the attached staff paper as their "policy bible" during future audits. While the staff paper is lengthy, a thorough review should answer any questions that you might have concerning the intent of the Board and the approach to be taken by the Audit Staff. Should you have any questions on the policy, please call Dave Mitchell at 202-324-2608.

Sincerely,

David F. Nemecek
Chief
National Crime Information Center

NCIC REGIONAL WORKING GROUP LIST

REGIONAL OFFICERS

NORTHEAST REGION

Chairman - John P. Cloherty 617-727-0090
Assistant Director FAX 617-232-1104
Executive Office of Public Safety
Criminal History Systems Board
1010 Commonwealth Avenue
Boston, MA 02215

1st Vice Chairman - Lieutenant Richard D. Boyden 802-244-8727 x220
Director FAX 802-244-1106
Vermont Criminal Information Center
Department of Public Safety
Post Office Box 189
Waterbury, VT 05676

2nd Vice Chairman - Mr. John B. Campbell 518-457-2393
Director, Data Processing FAX 518-457-3207
New York State Police
State Campus, Building #22
Albany, NY 12226

NORTH CENTRAL REGION

Chairman - Mr. Jack Pooler 517-336-6166
Executive Secretary FAX 517-336-6256
LEIN Policy Council
714 South Harrison Road
East Lansing, MI 48823

1st Vice Chairman - Mr. Richard V. White 217-782-4038
LEADS Administrator FAX 217-782-4036
Illinois State Police
P.O. Box 19461
301 Armory Building
Springfield, IL 62794-9461

2nd Vice Chairman - Mr. Carroll L. Bidler 515-281-8422
Administrator of Administrative Services FAX 515-242-6136
Wallace State Office Building
Des Moines, IA 50319

5/13/92

SOUTHERN

Chairman - Mr. Charles Pruitt 501-682-2222
Deputy Director FAX 501-682-7444
Arkansas Crime Information Center
One Capitol Mall, 4D-200
Little Rock, AR 72201

1st Vice Chairman - Mr. Brad Long 405-425-2224
Director FAX 405-425-2029
Oklahoma Law Enforcement
Telecommunications System
Post Office Box 11415
Oklahoma City, OK 73136

2nd Vice Chairman - Mr. Jose M. Camacho 305-471-1818
Information Systems Supervisor
Automated Systems Bureau
Metro Dade Police Department
9105 Northwest 25th Street
Miami, FL 33172

WESTERN

Chairman - Mr. David S. Gavin 512-465-2077
Chief, Crime Records Division FAX 512-465-2885
Texas Department of Public Safety
Post Office Box 4143
Austin, TX 78765-4143

1st Vice Chairman - Mr. James M. Wilson 307-777-7523
Communications Unit Supervisor FAX 307-777-7252
Division of Criminal Investigation
Criminal Justice Information Section
Rogers Building
316 West 22nd Street
Cheyenne, WY 82002-0001

2nd Vice Chairman - Mr. W. Gray Buckley 303-239-4224
Inspector FAX 303-235-0568
Colorado Bureau of Investigation
690 Kipling Street, Suite 3000
Denver, CO 80215

5/13/92

North Central Region Local Representatives

Deputy Chief Revel Brawner
Detroit Police Department
Management Services Bureau
1300 Beaubien
Detroit, MI 48226

313-596-1876
FAX 313-596-1605

Term expires June 30, 1993

Officer Gregory Canfield
Minneapolis Police Department
City Hall, Room 31
300 South 5th Street
Minneapolis, MN 55415

612-673-3336
FAX 612-673-2239

Term expires June 30, 1993

Major Leonard Ashworth
Topeka Police Department
204 Southwest 5th Street
Topeka, KS 66603

913-354-9445
FAX 913-354-9458

Term expires June 30, 1993

Mr. Terry Satterlee
Chief of Police
Sioux Falls Police Department
501 North Dakota Avenue
Sioux Falls, SD 57104

605-339-7261
FAX 605-331-2150

Term expires June 30, 1992

Lt. Col. Raymond B. Lauer
Bureau of Support Services
St. Louis Police Department
1200 Clark
St. Louis, MO 63103

314-444-5500
FAX 314-444-5958

Term expires June 30, 1992

Ms. Olivia Russell, Director
Records Division
Chicago Police Department
1121 South State Street, Room 206
Chicago, IL 60605

312-747-6258
FAX 312-747-5270

Term expires June 30, 1992

5/13/92

Northeast Region Local Representatives

Mr. Louis P. Chiarello
Acting Chief Communication Officer
Communications Department
Newark Police Department
31 Green Street
Newark, NJ 07102

201-733-8894
FAX 201-733-3984

Term expires June 30, 1993

Ms. Ann Marie Doherty
Deputy Superintendent
Operations Division Commander
Boston Police Department
154 Berkeley Street
Boston, MA 02116

617-247-4600
FAX 617-267-4360

Term expires June 30, 1993

Captain John Lytle
Warwick Police Department
99 Veterans Memorial Drive
Warwick, RI 02886

401-737-2244
FAX 401-738-1327

Term expires June 30, 1993

Major Peter C. Schaulis
Baltimore Police Department
601 East Fayette Street
Baltimore, MD 21202

301-396-2279
FAX 301-396-2108,
2109 or 2110

Term expires June 30, 1992

Captain Brian Craig
Commanding Officer, PCIC
Philadelphia Police Department
Franklin Square, Room 211
Philadelphia, PA 19106

215-592-5920
FAX 215-440-7915

Term expires June 30, 1992

Inspector John Gilmartin
Management Information Systems
New York City Police Department
1 Police Plaza, Room 700
New York, NY 10038

212-374-5020
FAX 212-693-2119

Term expires June 30, 1992

5/13/92

Western Region Local Representatives

Deputy Chief Duane Udland
Anchorage Police Department
4501 S. Bragaw Street
Anchorage, AK 99507

907-786-8552
FAX 907-786-8638

Term expires June 30, 1993

Mr. Joseph P. Bonino
Commanding Officer
Records and Identification Division
Los Angeles Police Department
150 N. Los Angeles Street, Room 210
Los Angeles, CA 90012

213-485-2601
FAX 213-237-0380

Term expires June 30, 1993

Mr. Donald N. Russell
Administrator
Records and Identification Bureau
Phoenix Police Department
620 West Washington Street
Phoenix, AZ 85003

602-262-7569
FAX 602-251-3958

Term expires June 30, 1993

Mr. Marvin R. Bullard
Deputy Chief of Police
Support Services Bureau
Dallas Police Department
2014 Main Street, Room 506
Dallas, TX 75201

214-670-3686
FAX 214-670-5661

Term expires June 30, 1992

Captain Gil Wright
Administrative Services
Ada County Sheriff's Department
7200 Barrister Drive
Boise, ID 83704

208-377-6704
FAX 208-377-6578

Term expires June 30, 1992

Mr. John Tomlinson
Police Systems Supervisor
Data Processing Section
Seattle Police Department
610 Third Avenue, Room 417
Seattle, WA 98104

206-684-5430
FAX 206-340-6048

Term expires June 30, 1992

5/13/92

Southern Region Local Representatives

Mr. Louie C. Caudell
Chief of Police
Little Rock Police Department
700 West Markham Street
Little Rock, AR 72201

501-371-4621
FAX 501-376-9552

Term expires June 30, 1993

Captain Kathy Witt
Fayette County Sheriff's Department
136 N. Martin Luther King Blvd.
Lexington, KY 40507

606-252-1771
FAX 606-259-0972

Term expires June 30, 1993

Sergeant W. G. Gordon
Communications Section
Atlanta Police Department
175 Decatur Street, SE
Atlanta, GA 30335

404-658-6700
FAX 404-681-0315

Term expires June 30, 1993

Mr. Joe Camacho
Metro Dade Police Department
Room 119
1320 Northwest 14th Street
Miami, FL 33125

305-471-1818
FAX 305-471-1878

Term expires June 30, 1992

Colonel Richard G. Engels
Chief of Police
Division of Police
Henrico County
Post Office Box 27032
Richmond, VA 23273

804-672-4840
FAX 804-672-5199

Term expires June 30, 1992

Captain Jim Tusan
Memphis Police Department
Room 12-23
201 Poplar Avenue
Memphis, TN 38103

901-576-2644
FAX 901-576-2635

Term expires June 30, 1992

5/13/92

NATIONAL CRIME INFORMATION CENTER

USER AGREEMENT

USER AGREEMENT

Responsibilities of Control Terminal Officer (CTO) in the National Crime Information Center (NCIC) System

I. Introduction

Since its inception, the NCIC has operated under a shared management concept between the FBI and state users. The NCIC Advisory Policy Board established a goal of having a single state agency in each state assume responsibility as the NCIC Control Terminal Agency (CTA) for the state, through and by which NCIC users in that state would access NCIC. The CTA is responsible for planning for necessary hardware, software, funding, and training for complete access to NCIC data services by all authorized agencies within the state.

The Board approved the CTA concept in order to unify responsibility for system user discipline, and adherence to system procedures and policies within each state. The CTA also serves as a central point in its state for handling record validations, quality control matters, dissemination of manuals and other NCIC publications, security matters, user training, audit, and any other problems concerning system use that may arise.

FBI NCIC responsibilities under this shared management concept includes provision of:

- operational, technical, and investigative assistance to NCIC users;
- telecommunications lines to a state interface;
- legal and legislative review of matters pertaining to NCIC;
- timely information on all NCIC aspects of system usage by means of the NCIC Operating Manual, Technical and Operational Updates, and related documents;
- staff research assistance;
- training and training materials to the control terminal agencies.

The responsibilities of the CTO and NCIC Service Coordinators (SC) are detailed in several documents related to the NCIC System. This agreement outlines the varied responsibilities of a CTO/SC as they pertain to the NCIC System.

The following documents are incorporated by reference and made part of this agreement:

- (A) National Crime Information Center Operating Manual.
- (B) NCIC Computerized Criminal History(CCH) Program Background, Concept and Policy as amended or superceded by implementation of the Interstate Identification Index (III) Program.
- (C) Minutes of the NCIC Advisory Policy Board.
- (D) Bylaws for the NCIC Advisory Policy Board and Regional Working Groups.
- (E) Title 28, Code of Federal Regulations, Part 20.
- (F) NCIC Standards as recommended by the NCIC Advisory Policy Board and approved by the FBI Director.
- (G) Applicable Federal and state law and regulation.

II.

Definitions

Control Terminal Agency

A CTA is a state or territorial criminal justice agency on the NCIC System providing statewide (or equivalent) service to its criminal justice users with respect to NCIC data. Only those agencies with direct telecommunications lines to NCIC may be control terminal agencies, and are held responsible for records entered through those lines. There will be no more than one CTA per state or territory.

NCIC Control Terminal Officer and Service Coordinator

An NCIC CTO shall be appointed by the head of each CTA.

An NCIC SC shall be non-CTAs which have direct NCIC telecommunications lines, which lines will be used only for system query functions.

The CTO will be allowed sufficient time to perform all necessary duties related to NCIC responsibilities. The CTO/SC and his agency will be responsible for

monitoring system use, enforcing system discipline, and assuring that NCIC operating procedures are followed by all users of the respective NCIC telecommunications lines as well as other related duties as outlined by this agreement. When a new CTO or SC is designated, the CTA head will notify NCIC of that appointment within 10 days of the appointment.

Timeliness

NCIC records must be entered promptly to insure maximum system effectiveness. A timely entry in the Wanted Person File is one made immediately once:

1. The decision to arrest or authorize arrest has been made; and,
2. The decision has been made as to whether and how far to go for extradition.

The date of want or date of warrant must be the date on which all those decisions were made.

A timely removal from the file means an immediate removal once the originating agency has documentation the fugitive has been arrested or is no longer wanted. Timely system inquiry means initiation of the transaction before an officer begins writing an arrest or citation document of any kind; storing inquiries when NCIC is down and submitting them at once when the system returns, regardless of whether the subject is still in custody; inquiry prior to the release of a person who has been incarcerated; and inquiry upon those who appear at a custodial facility to visit inmates.

Timeliness of entry/modification in the Missing Person File is generally the same as in the Wanted Person File.

Timely entry/modification of vehicle, license plate, and vehicle part data matches the wanted person standard, less the extradition considerations. Entry should be made as soon as a cross-checking with Motor Vehicles Registration Files has been completed.

Timely entry of gun, article, and securities information means within a few hours of the time complete information is available.

Validation

Validation (vehicles, plates, fugitives, missing person entries) obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation procedures are defined in Section IV-C of this agreement.

Completeness

Complete records of any kind include all information that was available on the person or property at the time of entry. The validation process should include a review of whether additional information has become available (missing from original entry) that could be added.

Complete inquiries on persons include numbers that could be indexed in the record; i.e., Social Security, Passport, VIN, License Plates, Driver's License, etc. Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

Accuracy

The accuracy of NCIC data must be double-checked by a second party. That verification should include assuring that the available cross-checks (VIN/license numbers) were made, and that data in the NCIC record matches the data in the investigative report. Agencies lacking support staff for this cross-checking should require the case officer to check the record, as he carries primary responsibility for seeking the fugitive and the stolen property.

III. Operational Responsibilities of Control Terminal Officers and Service Coordinators

To help ensure the proper operation of NCIC, the standards, procedures, formats, and criteria as contained in the NCIC Operating Manual will be followed. The CTA and its officers and their agencies with direct NCIC lines and their NCIC SCs must not only follow the rules as set forth, but also must ensure that agencies served by the control terminal do the same. Specific actions relative to two operational situations are:

(A) Ten Minute Hit Confirmation Policy

An originating agency must within ten minutes furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a notice of the specific amount of time necessary to confirm or reject.

This confirmation policy is especially critical with regard to a hit in the Wanted Person File. The NCIC Operating Manual describes procedures for handling a Wanted Person File hit in Part 7, Section 5.6. When an agency receives a hit on a wanted person record, it is requested by a caveat to "IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI." Confirming the hit means to verify with the ORI that the subject of the inquiry is identical to the subject in the record received, if the warrant is still outstanding, and whether or not the individual will be extradited. Upon receipt of a hit confirmation request, the originating agency must, within ten minutes, furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject. Therefore, in instances where the extradition information is not readily available, the originating agency should advise the inquiring agency, within ten minutes, that such is the case and how much time will be necessary to obtain the information.

An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to its CTO or SC and to the CTO or SC of the state in which the agency holding the record is located.

A CTO or SC designee of a system which services an originating agency of a record will institute appropriate action to ensure proper response to a hit confirmation request and to comply to system standards. This appropriate action may include canceling the record by the CTA.

Failure of a CTA to ensure compliance with this policy will result in imposition of sanctions as approved by the NCIC Advisory Policy Board.

(B) Control Terminal and/or NCIC Line Failure

Operational failure at the user end of an NCIC line may result from one of four conditions: (1) the NCIC computer is out of service; (2) the terminal equipment fails or is out of service; (3) a circuit or NCIC line problem; or (4) malfunction of terminal equipment. A terminal should make every effort to verify that the difficulty does not lie within its equipment. The CTA or SC should take the following action when in an out-of-service status and an analysis determines that the problem is not control terminal equipment difficulty: notify the local vendor providing communication service, log the time of notification, and note the circumstances relating to the problem. If, after a reasonable period of time, the vendor's efforts have not resolved the problem, notify FBI NCIC Headquarters and furnish the time the vendor was notified and a brief description of the problem.

IV. Quality Assurance Responsibilities

(A) Introduction

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. However, a CTA assumes a large degree of administrative responsibility and possible legal liability for

the maintenance of a criminal justice information system. This responsibility is being further defined by the courts. Accordingly, the CTA should institute appropriate and reasonable quality assurance procedures for all state system users. It appears from the cases reviewed that the courts have specifically addressed the issue as to whether criminal justice information system administrators (i.e., CTO and agency head) can be held liable for the negligent mishandling of a criminal justice record. In relation to 42 United States Code 3771, there is a standard which is prescribed for record management and (perhaps) the establishment of maintenance standards for these records. It can be said that criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up to date. To ensure reasonably sufficient record management, each CTA should ensure that there are security standards, audit standards, and personnel training standards which would allow accurate and up-to-date records and dissemination of the same.

(B) Record Quality

Errors discovered in NCIC records are classified as serious errors, form errors or an error trend.

- (1) Serious errors: NCIC will advise the CTA and the ORI via teletype message of an apparently erroneous record and request that it be verified, changed or canceled within 24 hours. If neither a response is received nor corrective action taken during that time, NCIC will cancel the record.
- (2) Form error or error trend: NCIC will mail a letter to the appropriate CTA. The CTA will forward a copy of the letter or a similar letter to the ORI so corrective action can be taken. No further notification or action will be taken by NCIC.

(C) Record Validation

NCIC periodically prepares listings of records on file for validation purposes. Validation listings are prepared pursuant to a schedule as published in the NCIC Operating Manual. These listings are mailed to the appropriate control terminals who in turn disseminate the records to the originating agency.

Each CTO will receive a letter explaining what records are contained in the validation, the order in which records are listed, and general procedures for validating the records. Also included are two letters which are to be executed by the NCIC CTO. One letter is used to acknowledge receipt of the validation material. This acknowledgement letter must be returned to FBI NCIC immediately. The second letter is for the CTO to certify that the records have been validated or that certification of validity has been received from the originating agencies.

Validation certification means that: (1) the records contained on the validation listing have been reviewed by the originating agencies; (2) the records which are no longer current have been removed from NCIC and all records remaining in the system are valid and active; (3) all records contain all available information; and (4) the information contained in each of the records is accurate.

This certification letter must be returned to the NCIC within 45 days from the date that the NCIC mailed the validations to the CTA.

If a CTA has not received a certification response from an agency under its service jurisdiction within a specified period of time, the CTA shall purge from NCIC all records which are the subject of that agency's validation listings. If a CTA fails to certify any validation listing to the NCIC within the specified time, all unvalidated records from that state will be purged by the NCIC.

V. Security Responsibilities

(A) General

The data stored in NCIC is documented criminal justice information and this information must be protected to ensure correct, legal and efficient dissemination and use. Information can be obtained from NCIC both directly and indirectly. Direct access is defined as terminal access and dissemination within that terminal agency. Indirect access is nonterminal access outside of an agency with direct access.

There is no Federal legal or policy prohibition against indirect dissemination of information contained in NCIC, other than criminal history record information. If no state/local law or policy prohibition exists, indirect dissemination of NCIC records, other than criminal history record information, is discretionary with the CTA. Such information may be withheld because of criminal justice priorities, budgetary limitations, or other reasons determined to be legitimate by the CTA.

An agency participating in the NCIC as a CTA and other agencies with direct telecommunications line access must assume responsibility for and enforce system security with regard to all other agencies which it in turn services.

Security guidelines relating to criminal history record information are set forth in the NCIC CCH Program Background, Concept and Policy as superseded by the III Program and in Title 28 Code of Federal Regulations Part 20, Subparts A and C.

(B) Originating Agency Identifier (ORI)

An NCIC ORI is a nine character identifier assigned by FBI NCIC to an agency which has met the established qualifying criteria for ORI assignment to identify the agency in transactions in the NCIC System. The assignment of an ORI to an agency is not a guarantee of access to the NCIC System. The ultimate decision regarding who may access NCIC lies with the CTA.

A CTO shall coordinate the assignment of new ORI numbers, the change in ORI location or address, any other changes, cancellations, or retirements of ORIs accessing NCIC through the CTA system with the FBI NCIC. The CTO will submit necessary documentation when requesting the assignment of an ORI. This documentation should include a statute or executive order which indicates an agency is governmental and performs the administration of criminal justice. A statement should be included that indicates that an agency allocates more than 50% of its annual budget to the administration of

criminal justice. If the agency is under the management control of a criminal justice agency, a copy of the management control agreement should be submitted. Assignment of ORIs to agencies with special or limited NCIC access will also be coordinated by the respective CTOs.

Validation

Each ORI accessing NCIC shall be validated on a biennial basis by the CTO. A printout containing ORIs of agencies accessing NCIC through the state system is forwarded to the CTO who shall check the accuracy of each ORI listing to include verification of:

- agency type code.
- agency name and locality.

The CTO shall certify that all ORIs are valid and correct as listed.

VI. Computerized Criminal History Record Information Responsibilities

- (A) Each CTA shall conform with system policy as established by the NCIC Advisory Policy Board and approved by the FBI Director before being permitted access to criminal history record information. This conformity will allow for control over the data and give assurance of system security.
- (B) Each CTA is responsible for the security throughout the system being serviced by that agency, including all places where terminal devices are located. Upon determination that a terminal is in nonconformance with system management or security policy, the CTA shall cause that terminal's access to NCIC to be disabled.
- (C) A system security officer shall be designated in each CTA to assure all necessary physical, personnel, computer, and communication safeguards prescribed by the Board are functioning properly in systems operations.
- (D) The rules and procedures governing direct terminal access to criminal history record information shall apply equally to all participants to the system, including the state CTAs and SCs, Federal SCs, and other agencies having access to the data stored in the system.

- (E) All CTAs and other criminal justice agencies having direct access to computerized CHRI data from the system shall permit an NCIC audit team to conduct appropriate inquiries with regard to any allegations of security violations.
- (F) The CTA shall define procedures to ensure all satellite computers and all remote terminals accessing criminal history record information through the state system will maintain a manual or automated dissemination log with notation of the individual making the request for the record. All logs will be maintained for a minimum of one year.
- (G) A CTA will ensure that all computers and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history record information must be under the management control of a criminal justice agency as defined by the NCIC CCH background and policy document.

All CTAs and SCs should institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of information in the system. These self-audits should be on a continual basis to ensure both quality assurance and compliance with standards.

In addition to audits conducted by all CTAs and SCs, each CTA/SC shall be audited at least once every two years by the NCIC Staff. This audit shall include a sample of state and local criminal justice agencies. The objective of this audit is to verify adherence to NCIC policy and regulations and is termed a compliance audit. In order to assist in this audit, each CTO and SC will respond to a preaudit questionnaire which will serve as the audit guideline. A compliance audit may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance.

Such compliance audits shall cover the following areas in connection with both the III and NCIC stolen property and person records:

Accuracy

That any NCIC entry shall contain no erroneous data. In addition, CTAs/SCs should maintain necessary documentation as required by

NCIC policy. They should also ensure that documentation is available from state and local users accessing NCIC through them.

Completeness

That information contained in an NCIC entry or in a criminal history record to be disseminated is all the pertinent available information.

Timeliness

That entry, modification, update, and removal of information are completed as soon as possible after information is available and that information is processed and transmitted in accordance with standards as established by the Board.

Security

The ability of an organization to protect its information against unauthorized access, ensuring confidentiality of the information in accordance with laws and with NCIC policy, regulations, and standards.

Dissemination

That all information released is in accordance with applicable laws and regulations and that a record of dissemination of criminal history records is maintained.

In addition, CTAs/SCs should also ensure that documentation is available from state and local users to assist in both the self-audit and national audit programs.

VII. Administrative Responsibilities

- (A) Each state CTO shall serve as a representative of his/her state to the Regional Working Group (RWG) meetings. The state CTO may designate someone in his/her state to attend and vote at the RWG meetings.

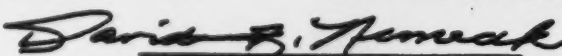
The state CTO shall provide to the RWG chairperson, upon request, a list of those items pertaining to the operation of the NCIC System as well as suggestions for improvement in the operations of the NCIC System which may require discussion at the RWG meetings.

Consistent with each CTO's responsibility to represent the users of that state, he/she should distribute those items on the agenda to be discussed at a RWG meeting to appropriate state and local users to ensure that all views on the topics are obtained and represented. In addition, he/she should be prepared to fully discuss those agenda items at the RWG meetings.

- (B) The CTO shall cooperate, to the maximum extent possible consistent with any fiscal, time, or personnel constraints, in the response to requests for information in the form of surveys, questionnaires, or similar methods, which may be provided by FBI NCIC from time to time.
- (C) The CTO shall be responsible for providing adequate training to agencies accessing NCIC through the state CTA computer.
- (D) The CTO shall ensure that publications emanating from FBI NCIC be distributed to appropriate personnel in that state. Consistent with this provision, the CTO shall coordinate distribution within their state criminal justice community of the NCIC Technical and Operational Update, NCIC Operating and Code Manuals, and, as requested, miscellaneous publications in order to enhance effective use of the NCIC System

ACKNOWLEDGMENT

As a CTA/SC serving in the NCIC System, we hereby acknowledge the duties and responsibilities as set out in this document as well as those documents incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved by NCIC System users in order to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the NCIC System. We further acknowledge that a failure to comply with these duties and responsibilities will subject my state system and those other state and local criminal justice users accessing NCIC through that system to various sanctions as approved by the NCIC Advisory Policy Board. These sanctions may include the termination of NCIC services to the CTA.

Service Coordinator	Date	Service Coordinating Agency Head	Date
			
Chief, FBI NCIC		Date	

The network philosophy of the State Control Terminal Agency (SCTA) is a sound one but has not been fully implemented. The negative result of this delayed implementation has been counter to the expressed NCIC purpose to "help the criminal justice community" perform its duties. In effect, certain cities in our present network configuration are being helped to the disadvantage of the SCTA; and indirectly are being helped to the disadvantage of other agencies nationwide that must rely on the SCTA system to enforce discipline.

Effective operation of the NCIC System and effective communications throughout the networks within each state are not possible under the present condition. Criminal justice agencies cannot rely on the present design to aid them in ensuring that their communications have followed all the necessary channels in the most effective manner. Most SCTAs have and/or have access to more data files than are available in NCIC. For example, in addition to forwarding wanted person inquiries to NCIC, SCTAs also search state wanted files to obtain misdemeanor warrant entries which do not qualify for entry in NCIC. Some SCTAs forward stolen vehicle inquiries to NCIC, state vehicle files, and computerized motor vehicle registry files and provide the inquiring officer with not only the results of the stolen check, but also the name, address, etc., of the registered owner. Some SCTAs may carry the last example another step and provide the officer with any warrants issued for the registered owner. Thus, the use of a direct line between the NCIC System and a city/regional system also results in the criminal justice officer losing services which are available at, and provided by, only the SCTA.

System discipline, standards, management, and control are subverted by the present fragmented arrangement and the result hinders interagency cooperation.

The use of "effective communications" to help the criminal justice community perform its duties not only means providing access to and detailed information from pertinent computerized data bases, but also includes the amount of time required to access the data bases. While an entry, inquiry, or update message may contain specific and detailed information, the message (communication) could be very ineffective if it cannot be transmitted to the data center, and a response received from the data center within a reasonable amount of time. It is not uncommon to hear of a hit occurring minutes after the record was entered. Restrictions have also been placed on the amount of time that a person may be detained while an inquiry is being made to determine whether a record is on file in a data base. The rapid transmission of messages is extremely important and the standards

were prepared to ensure that messages are transmitted and processed within a reasonable amount of time.

Neither the NCIC System nor the state networks will ever be able to reach their maximum potential as criminal justice tools until all the necessary components are working toward that end. Until then the effectiveness of the entire effort is diminished.

There are currently a number of NCIC lines which go directly to city and regional computer systems and FBI field offices. Many of these direct lines have a very low volume of traffic. In these times of fiscal constraints, unnecessary and/or exorbitant costs are inexcusable. Under what situations do direct lines to city/regional systems exist? Study reveals that, while many situations may first appear to be unique, the reasons in fact can be categorized into one or more of the following areas of complaint:

1. Satisfactory response time is not provided by the SCTA.
2. System availability is not satisfactory.
3. Some services provided by NCIC are not available through the SCTA.
4. Equipment and/or technical methods are incompatible with the SCTA.

Reaching the objective to provide the most reasonably effective communications network for all criminal justice agencies will not be possible unless the direct lines to city/regional systems and FBI field office arrangements are eliminated and the needs of everyone involved are properly met.

To accomplish this objective the establishment of certain policies and standards must be completed, adopted, and followed. Through these policies and standards a tool of measurement will be provided against which the Advisory Policy Board can measure the performance of the component parts of the system as a whole. These policies and standards also must address the specific areas of complaint of the "special" case situations.

For the purposes of the standards on the following pages, any 1200 or higher baud line shall be considered a high-speed line.

STANDARDS FOR INQUIRY RESPONSE TIME - HOT FILES (NON-III)
High-Speed Line - Computer Interface

1. Average message response time for an inquiry from the SCTA to NCIC and back to the SCTA should not exceed two seconds.
2. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 12 seconds after transmission of the inquiry, with two of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1 above.
3. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 22 seconds after the transmission of the inquiry, with 12 of the 22 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 1 and 2.
4. Average response time from any local/regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 12 seconds, with two of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1.
5. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the inquiry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 12 second response time indicated in standard 2 above.

Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the one-month compilation.

STANDARDS FOR RESPONSE TIME (III)
High-Speed Line - Computer Interface

1. Average message response time for an inquiry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.
2. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 15 seconds after transmission of the inquiry, with five of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1 above.
3. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 25 seconds after the transmission of the inquiry, with 15 of the 25 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 1 and 2.
4. Average response time from any local regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 15 seconds, with five of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1.
5. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the inquiry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 15 second response time indicated in standard 2 above.

Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as the installation of a new computer, should be excluded from the one-month compilation.

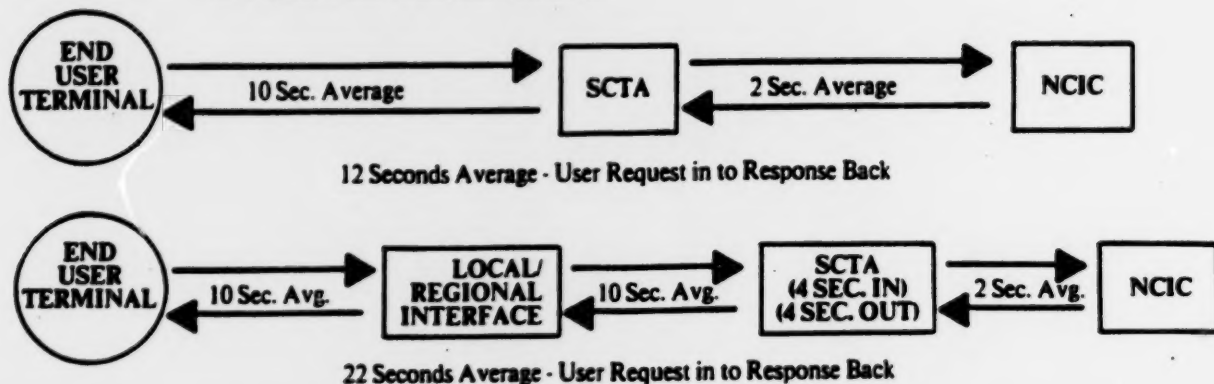
STANDARDS FOR RECORD ENTRY BY USER AGENCY

1. Any agency having investigative authority and jurisdiction and having an NCIC-assigned Originating Agency Identifier (ORI) must enter records into NCIC which meet NCIC criteria as soon as reasonably possible after minimum information is available.
2. The SCTA shall be responsible for assuring that every agency which has a terminal or access to a terminal by some interagency agreement and has an NCIC-assigned ORI and investigative authority and jurisdiction may enter records into NCIC.
3. Every agency which enters records destined for NCIC must assure that "hit" confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location.
4. Every agency is responsible for the removal of its NCIC record as soon as it is aware that the record is no longer valid.
5. Average message response time for an entry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.
6. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 20 seconds after transmission of the entry, with five of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 5 above.
7. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 35 seconds after the transmission of the entry, with 20 of the 35 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 5 and 6.
8. Average response time from any local/regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 20 seconds, with five of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 5.

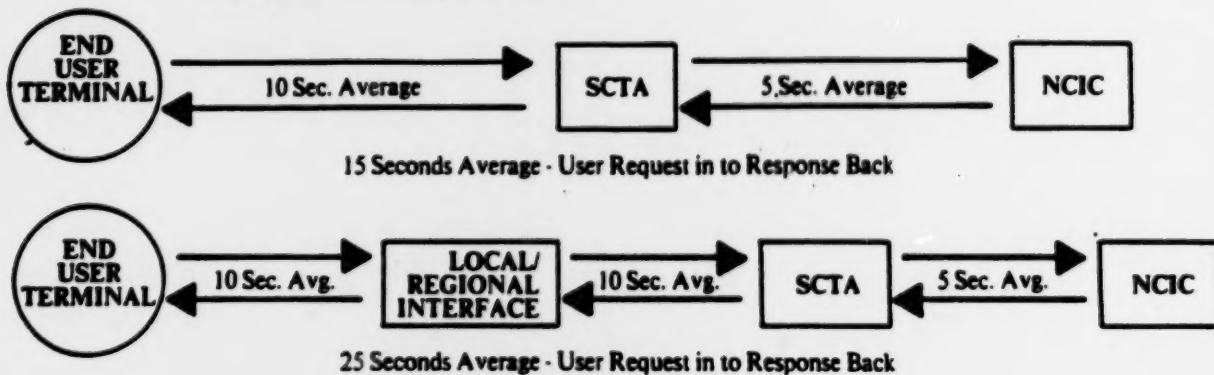
9. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the entry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 20 second response time indicated in standard 6 above.

Standards for record entry into NCIC for processing are shown in Example C.

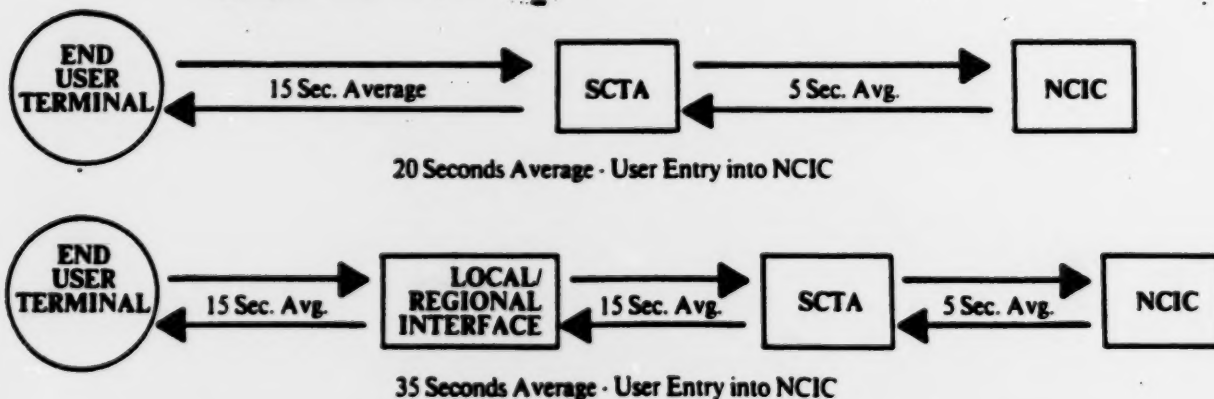
EXAMPLE A: NCIC Inquiries - Hot Files
High Speed Lines - Computer Interfaces



EXAMPLE B: NCIC Inquiries - III
High Speed Lines - Computer Interfaces



EXAMPLE C: NCIC Record Entry
High Speed Lines - Computer Interfaces



Note: Times shown above should be considered maximum. In many cases, time will be less depending on individual computer systems being used. All times should be considered on an average when all systems are operating normally. Average time should be based upon a compilation over a one-month period.

STANDARDS FOR AGENCIES RECEIVING A POSITIVE RESPONSE (HIT)

1. Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions based upon the hit NCIC record: (1) arresting the wanted person; (2) detaining the missing person; or (3) seizing the stolen property.

Confirming a hit means to contact the agency that entered the record to:

- A. Ensure that the person or property inquired upon is identical to the person or property identified in the record;
 - B. Ensure that the warrant, missing person report, or theft report is still outstanding; and,
 - C. Obtain a decision regarding (1) the extradition of a wanted person, (2) information regarding the return of the missing person to the appropriate authorities, or (3) information regarding the return of stolen property to its rightful owner.
2. Every agency upon taking a person into custody or acquiring property, after confirming the hit, must place a locate on the corresponding NCIC record(s).

STANDARDS FOR SYSTEM AVAILABILITY

The NCIC Computer availability goals shall be 100% with 99% as minimum acceptable performance.

The SCTA computer availability goals shall be 100% with 96% as minimum acceptable performance.

The local/regional computer availability goals shall be 100% with 96% as minimum acceptable performance.

STANDARD REGARDING EQUIPMENT AND TECHNOLOGY COMPATIBILITY

Equipment and/or technological incompatibility shall not be sufficient justification for any agency to operate outside of the normal SCTA configuration.

STANDARDS FOR SERVICES AVAILABILITY

Those services provided by NCIC to the SCTAs shall be provided by the SCTAs to their users with the exception of:

- (1) Services specifically limited to SCTAs by NCIC policy; and
- (2) Services which are restricted to certain users by nature of their governmental and/or criminal justice status and the Federal laws and regulations governing access to certain types of NCIC services.
- (3) Services which may be contrary to a state law or executive order.

"Users" include those agencies having a direct telecommunications link with an SCTA, and any regional dispatch center, electronic switcher, satellite computer, or other computer interface, providing a telecommunications link to user agency as well as those agencies who have no telecommunications link but access an SCTA via another user which has a telecommunications link. Any regional dispatch/communication center shall be required by the SCTA to provide the same services to their users as those provided to them by the SCTA.

Services include:

1. Providing users with the capability of communicating with and receiving responses from all current and future NCIC Files.
 - Article
 - Boat
 - Canadian Warrant

- Gun
 - Interstate Identification Index (III) including the NCIC Federal Offenders File and the FBI Automated Identification Division System (AIDS)
 - License Plate
 - Missing Person
 - Securities
 - Unidentified Person
 - U.S. Secret Service Protective
 - Vehicle
 - Wanted Person
 - ZO
2. The capability to enter an NCIC record into all current and future NCIC Files which:
 - A) Meets the NCIC entry criteria for the file involved;
 - B) Contains at least the minimum data required by NCIC for entry and up to the maximum number of identifiers permitted in the record by NCIC; and
 - C) Contains any of the codes or data permitted by NCIC in each of the fields.
 3. Entry of a valid record shall be permitted regardless of the existence of any other record(s) already entered in NCIC by any other agency(s) for the person or property in question.
 4. The capability to add information to, delete information from, and/or change information in a field(s) of an existing NCIC record.
 5. The capability to remove a record from file when a record is determined to be invalid, e.g., the warrant which was the basis for an entry is dismissed, or when the person or property which is the subject of the record is found.
 6. The capability to place a locate against another agency's NCIC record, including records entered by agencies serviced by the same SCTA as well as records entered by agencies serviced by another SCTA.

The use of the above services by any user agency shall be in accordance with the instructions and procedures contained in the NCIC Operating Manual, the codes contained in the NCIC Code Manual, and new enhancements contained in the NCIC Technical and Operational Update, NCIC Newsletter, or any other official notification from FBI NCIC.

SANCTIONS

Purge of an agency's NCIC records and discontinuance of System access for an agency are the two ultimate sanctions available to NCIC management for enforcement of System policy and procedure. This presumes prosecution for law violations would normally be handled at the state level, directed toward an individual rather than toward an agency.

Inflexible procedures for policy enforcement would be a hinderance to good NCIC management. We recommend, instead of rigid enforcement of the established rules, that NCIC in concert with the CTAs, Regional Working Groups, and the Board utilize the sanctions identified below in a reasonable way to gain compliance with System objectives. Usually problems of a serious nature are corrected quickly through telephone conversations among the parties involved. Each case has peculiarities of its own.

These sanctions should be viewed as part of the package of an improved user agreement and proactive quality assurance measures. It is unlikely a notice of caution would ever be sent to the chief executive of a state. Should it become necessary, however, the Board must make it clear now to every CTA and to NCIC that the Board finds such action reasonable and necessary, and supports FBI enforcement of established NCIC policy.

References to CTAs throughout this report include "other agencies with direct NCIC lines" when the inclusion is logical.

Considerations

1. An up-to-date NCIC/CTA user agreement should be on file with the NCIC Section (copy with CTA) and it should include reference to the sanctions that could be imposed for failure to comply.
2. Specific references should include but not be limited to:
 - Failure to react properly to error notices
 - Failure to react properly to hit confirmation requests
 - Failure to locate
 - Failure to complete entries/modifications/removals promptly

- Failure to make complete entries
 - Failure to validate
 - Failure to assure security of equipment and data
 - Failure to provide qualified operators
 - Entry of invalid or nonqualified records
3. A special audit of a CTA should be part of the sanction package.
 4. Flagging records of substandard CTA lines should be an option.
 5. Deadlines should be imposed on compliance with corrective action notices.
 6. Letters to CTAs, rather than being titled "Caution" should be drafted in the framework of a "request to comply" with NCIC Standards. When prolonged failure to comply would result in discontinuance of service, the letter should be explicit in announcing the "probationary" status of the CTA; or in announcing the date probationary status will begin if compliance is not forthcoming before then.
 7. Unless the serious nature of a problem requires immediate discontinuance of service, a letter to the Governor should precede discontinuance of service.

I. NLETS message transmitted by FBI NCIC to control terminal agency for all nonserious errors

A. Redirection of NLETS message by CTA to offending terminal agency. (CTA to maintain copy of these messages for follow up.)

II. Verbal notice from CTA to terminal agency for nonserious error intercepted by CTA

or

Intrastate message to offending terminal agencies for nonserious errors or reports thereof. (Note: record of verbal notices should be retained by CTA for six months.)

III. Letter of request for compliance

A. FBI NCIC to CTA officer regarding:

1. Untimeliness
2. Inaccuracy
3. Incompleteness
4. Unsatisfactory record quality
5. Unsatisfactory validation
6. Misuse of system
7. Notice of probationary status resulting from audit
 - a) 30 days to correct deficiencies
8. Serious Error

B. CTA to terminal agency

1. Untimeliness
2. Inaccuracy
3. Incompleteness

III. Letter of request for compliance - (cont.)

4. Unsatisfactory record quality
5. Unsatisfactory validation
6. Misuse of system
7. Notice of probationary status resulting from audit
 - a) 30 days to correct deficiencies
8. Serious error

IV. Letter of intent to remove from system if deficiency not corrected

A. Board to CTA head

1. Continuous serious error trend
2. Audit failure status (not corrected within 30 days of first letter of request)
3. Intentional misuse of "PUR/C" Code in III

B. CTA to terminal agency

1. Continuous serious error trend
2. Audit failure status (not corrected within 30 days of first letter of request)
3. Intentional misuse of "PUR/C" Code in III

V. Advisory letter to governor

A. FBI NCIC to governor with copy to CTA

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probationary status has been modified to failure status (additional 30 days to correct)
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

- B. CTA to terminal agency - removal of records and discontinuance of service is imminent

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probation status to failure status
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

VI. Removal from system includes purge of all records and discontinuance of service pending reinstatement

- A. Board and FBI NCIC jointly initiate removal of CTA/state from active system use
- B. CTA may discontinue service to an offending agency, and purge that agency's records from state and NCIC files

VII. Reinstatement

- A. Upon satisfactory proof the offending state has corrected its deficiencies the Board may reinstate
- B. Upon satisfactory proof offending terminal has corrected its deficiencies CTA may reinstate. CTA also has option to defer to another agency who would become the CTA



National Crime Information Center

Computerized Criminal History Program

Background, Concept and Policy

SMC-HD #5

142

For Official Use Only

*Approved by the NCIC
Advisory Policy Board
March 1, 1984*

BACKGROUND AND CONCEPT

The establishment in 1971 of the Computerized Criminal History (CCH) File as part of the operating NCIC System was a major step forward in making this system of optimum value to all agencies involved in the administration of criminal justice. Offender criminal history has always been regarded by NCIC as the basic file in a criminal justice information system. From the beginning of NCIC, the sensitivity of a criminal history file with its security and confidentiality considerations has always been recognized (Science and Technology Task Force Report, The President's Commission on Law Enforcement and Administration of Justice, 1967).

It is important to keep in mind the need to develop an offender criminal history exchange with the states that will rapidly gain the confidence of all users in terms of system integrity, accuracy, and completeness of file content. This type of discipline is necessary if a nationwide system employing the necessary standards is to succeed. Such discipline is an essential consideration during the record conversion stage, even though available data is limited, and becomes an essential goal in an operating on-line system.

From its inception, the concept of NCIC has been to serve as a national index and network for 50 state law enforcement information systems. Thus, the NCIC does not, nor is it intended to, eliminate the need for such systems at appropriate state and metropolitan levels, but complements these systems. The concept was built on varying levels and types of information in metropolitan area, state, and national files. In such an overall system, many thousands of duplicate indices in local, state, and Federal agencies could be eliminated and all agencies share in centralized operational information from a minimum number of computer files. The purpose of centralization beyond economics is to contend with increasing criminal mobility and recidivism. Computer and communications technology makes this possible and, in fact, demands this system concept.

Our way of life demands that local and state governments retain their traditional responsibility over law enforcement. Computer and communications technology such as NCIC enhances local and state capability to preserve this tradition. The NCIC System places complete responsibility for all record entries on each agency--local, state, and Federal. Likewise, clearance, modification, and cancellation of these records are also the responsibility of the entering agency. Each record, for all practical purposes, remains the possession of the entering agency. However, each local and state agency in one state can immediately share information contributed by another agency in

another state. This continuity of information greatly increases the capability of local and state agencies in working across state lines, which have in the past been barriers to mutual state and local law enforcement efforts.

The NCIC System, which is the first use of computer/communications technology to link together local, state, and Federal governments, established the control terminal concept. In a national system, although the individual users are responsible for the accuracy, validity, and completeness of their record entries and their action decisions on positive responses to inquiries, more stringent controls with respect to system discipline are required. A control terminal on the NCIC System is a state agency or a large core city servicing state-wide or metropolitan area users. These control terminals, rapidly becoming computer based, share the responsibility in the national network for monitoring system use, enforcing discipline, and assuring system procedures and policies are met by all users. The NCIC System, through its related control terminals and the advent of criminal history, has a potential of over 64,000 local, state, and Federal criminal justice user terminals. Tradition, computer/communications technology, and the potential size of the NCIC network and its related state systems demand that its management responsibility be shared with the states. To accomplish this objective, an NCIC Advisory Policy Board was established.

From the beginning, the NCIC System concept has been to encourage and develop strong central state information and communications services. Through mandatory reporting laws at the state level, essential centralized files can be established for both operational and administrative use. The administrative or statistical use of computer-based files is a vital consideration. A state cannot make intelligent decisions about crime problems or criminal justice effectiveness unless it can statistically document the extent and nature of crime and the success or failure of the criminal justice system in its treatment of offenders. Thus, the planning of these systems must incorporate means of obtaining the necessary statistical data as a byproduct of the operational information being processed on a day-to-day basis. This is particularly true with respect to the criminal history application.

Of additional significance is a standardized law enforcement statistics program entitled "Uniform Crime Reports." Historically, this program collected crime statistics directly from individual law enforcement agencies. For several years the program has embarked on an effort to assist the various states in

creating their own statistical program. As of 1978, there were 43 states collecting crime statistics through a central state collection agency. The state programs provide the FBI with the necessary information to compile a national view of crime.

Offender criminal history, i.e., the physical and numerical descriptors of an arrested person and the basic recorded actions of the criminal justice agencies with respect to the offender and the charge, is vital information in day-to-day criminal justice operations. An FBI study entitled "Careers in Crime," published annually through the Uniform Crime Reporting Program, documents on a limited basis the extent of criminal repeating by the serious offender. Recent analysis indicates the number of years between the first and last (most recent) arrest was five years and five months and that within that time span the criminal repeater, measured on the basis of arrest, was arrested four times. A further study indicates 49 percent of persons arrested more than once were rearrested within the same state. When individuals having only one arrest are considered, then 67 percent of all the persons arrested were arrested within a single state. Therefore, an offender criminal history file in scope and use is essentially a state file and a state need.

There is, however, substantial interstate criminal mobility (33 percent) which requires sharing of information from state to state. There is no way to positively identify a first offender who will later commit a crime in another state. The approach then to a national index must be an empirical judgment that all state offenders committing serious and other significant violations must be included in the national index. As in other aspects of the system, the determination of which criminal acts constitute serious or significant violations resides with each individual state. A national index is required to efficiently and effectively coordinate the exchange of criminal history among state and Federal jurisdictions and to contend with interstate criminal mobility.

The development of offender criminal history for interstate exchange required the establishment of standardized offense classifications, definitions, and data elements. Felony and misdemeanor definitions cannot be used in this approach because of the wide variation in state statutes. In fact, the definitions of a specific crime by state penal codes also vary widely. For full utility and intelligent decision-making, offender criminal history requires a common understanding of the terminology used to describe the criminal act and the criminal justice action.

Each computerized offender criminal history cycle must have a criminal fingerprint card as its basic source document. This is necessary in order to preserve the personal identification integrity of the system. While the criminal

history file in the NCIC System will be open to all criminal justice terminals for inquiry, only the state agency can enter and update a record. This procedure provides for better control over the national file and its contents. It relies on a central state identification function to eliminate duplication of records and provides the best statistical opportunity to link together multijurisdictional criminal history at local and county levels.

Using the NCIC concept of centralized state information systems, another requirement is to change the flow of criminal fingerprint cards. Local and county contributors within a state must in an ultimate operational system forward criminal fingerprint cards to the FBI through the central state identification function. Where the state can make the identification with a prior print in file, it can take the necessary action in a computerized file without submission to the FBI. Where the state cannot make the identification, the fingerprint card must be submitted to the national identification file. Again, the system's concept is that a fingerprint card must be the source document for a record entry and update, but now it will be retained at the state or national level. This approach eliminates considerable duplication of effort in identifying fingerprint submissions, particularly criminal repeaters at state and national levels. It will be the responsibility of each state to determine its own capability in regard to servicing intrastate criminal fingerprint cards. Whenever a state has determined that it is ready to assume processing all intrastate criminal fingerprint cards, the state agency will inform contributors within the state to forward to the state identification bureau all criminal fingerprint submissions, including those which were previously directed to the FBI, and will also so inform the FBI. Since the success of the system concept depends on this procedure, all possible measures will be taken to assure compliance.

The justification for a national index is to efficiently and effectively coordinate 50 state systems for offender criminal history exchange. The need is to identify the interstate mobile offender. FBI statistics with respect to more serious offenders indicate that about 67 percent confine their criminal activity to a single state. These are categorized as single-state offenders. Therefore, 33 percent commit crimes, are arrested, and are fingerprinted in two or more states. These are categorized as multistate offenders.

In either event sufficient data must be stored in the national index to provide all users, particularly those users who do not have the capability to fully participate in the beginning system, the information necessary to meet basic criminal justice needs.

In order for the system to truly become a national system, each state must create a fully operational state computerized criminal history capability with the state.

Although the present need for the criminal history file and the unequal development of state criminal justice systems dictate a simple initial index structure, the ultimate system should differentiate between multistate and single-state offenders with respect to the level of residency of detailed criminal history. Single-state offenders are those whose criminal justice interactions have been non-Federal and confined to a single state having a computerized criminal history system.

The interstate exchange of computerized criminal history records requires a standard set of data elements and standard definitions. The system design was built upon user needs for all criminal justice agencies and ends with user input. It was designed not only on what is possible to achieve in the future, but also to operate on the information and hardware available at all levels at the present time. While the formats and standardized offense classifications and definitions seem ambitious, to implement a system of this potential scope and size without a design to substantially improve the identification/criminal history flow would be a serious error.

System Concept

As pointed out earlier, the concept of NCIC since initial planning in 1966 has been to complement state and metropolitan area systems. Although computer/communications technology is a powerful tool, a single national file of detailed law enforcement data was viewed as being unmanageable and ineffective in serving the broad and specialized needs of local, state, and Federal agencies. The potential size and scope of a national system of computerized criminal histories involving 60,000 criminal justice agencies demand joint management by the states and the FBI NCIC.

Necessity for State Files

(1) Sixty-seven percent of the criminal history records will be single state in nature, i.e., all criminal activity limited to one state and, therefore, the responsibility of and of primary interest to that state.

(2) State centralization can tie together the frequent intrastate, multijurisdictional arrests of the same offender and thus eliminate unnecessary duplication of files at municipal and county levels. This will obviously result in economies.

(3) A state system with a detailed data base, because of its manageable size, can best satisfy most local and state criminal justice agency information needs both on and off line. The national file then complements rather than duplicates the state file.

(4) A state with a central data base of criminal history has the necessary statistical information for overall planning and evaluation, including specialized needs unrelated to the national file.

(5) State control of record entry and updating to the national file more clearly fixes responsibility, offers greater accuracy, and brings about more rapid development of the necessary standards.

(6) A central state system provides for shared management responsibility with FBI NCIC in monitoring intrastate use of the NCIC, including security and confidentiality.

(7) Channeling the criminal identification flow through the state to the national level eliminates substantial duplication of effort at national and state levels.

Compatibility of State and National Files

(1) To contend with criminal recidivism and mobility, a national index of state and Federal offender criminal history is necessary, i.e., a check of one central index rather than 51 other jurisdictions.

(2) The duplication provides a backup to recreate either a national or state file in the event of a disaster, a cross-check for accuracy, validity, and completeness as well as a more efficient use of the network.

(3) The NCIC record format and data elements for computerized criminal history afford a standard for interstate exchange.

(4) In the developed system, a single-state record (67 percent) will become an abbreviated criminal history record in the national index with switching capability for the states to obtain the detailed record. Such an abbreviated record should contain sufficient data to satisfy most inquiry needs, i.e., identification segment, originating agency, charge, date, disposition of each criterion offense, and current status. This will substantially reduce storage costs and eliminate additional duplication.

Program Development

The proper development of the Computerized Criminal History Program, in terms of its impact on criminal justice efficiency and effectiveness and dollar costs, is vital. At the present time, there is a wide range of underdevelopment among the states in essential services such as identification, information flow, i.e., court disposition reporting programs, computer systems, and computer skills.

(1) NCIC implemented computerized criminal history in November, 1971, requiring the full interstate format for both single and multistate records because:

- (a) This enables all states to obtain the benefits of the Computerized Criminal History Program.
- (b) This provides all states time to develop and implement the necessary related programs to fully participate.
- (c) Familiarity with and adherence to all system standards will speed program development.

(2) It is understood that the NCIC Computerized Criminal History Program will be continually evaluated, working toward the implementation of the single-state, multistate concept.

Levels of Participation

(1) The state maintains a central computerized criminal justice information system interfaced with NCIC. The state control terminal has the on-line capability of entering new records into state and NCIC storage, as well as the ability to update the computer-stored records. Through the state system local agencies can inquire on line for criminal history at state and national levels. This is a fully participating NCIC State Control Terminal Agency (SCTA).

(2) The state maintains an electronic switch linking local agencies for the purpose of administrative message traffic and on-line access to NCIC through a high-speed interface. No data is stored at state level; however, criminal history records are stored in NCIC, and new records are entered and updated by the SCTA from a manual interface to the electronic switch. The switch provides local agencies direct access to NCIC for criminal history summary information and other files.

(3) The state maintains a manual terminal on low-speed line to NCIC. The SCTA services local agencies off line, e.g., via radio, teletype and telephone. Since the volume of computerized criminal history is relatively small, the SCTA may convert criminal history records, enter and update these records in NCIC. There is no computer storage at state level.

Levels 2 and 3 are interim measures until such time as the state agency secures the necessary hardware to fully participate. At that time, the state records stored in NCIC will be copied in machine form and returned to the originating state to implement the state system.

SECURITY AND CONFIDENTIALITY

This section, Security and Confidentiality, shall apply to the NCIC Interstate Identification Index (III). The III shall include the Index in NCIC to state and Federal criminal history records as well as criminal history record inquiries and requests via NCIC telecommunications lines and subsequent responses from:

- o the Index
- o the NCIC Federal Offender File
- o the FBI Automated Identification Division System (AIDS)
- o the files of III participating state agencies

When the phrases "Computerized Criminal History File," "interstate criminal history exchange system," or the abbreviation "CCH" appear, the phrase "Interstate Identification Index," or the abbreviation "III" should be substituted.

I. Information in FBI NCIC Interstate Criminal History Exchange System

- A. Entries of criminal history data into the NCIC computer and updating of the computerized record will be accepted only from an authorized state or Federal criminal justice control terminal. Terminal devices in other criminal justice agencies will be limited to inquiries and responses thereto. An authorized NCIC State Control Terminal Agency (SCTA) is defined as a state criminal justice agency on the NCIC system servicing statewide criminal justice users with respect to criminal history data. Control terminals in Federal agencies will be limited to those involved in the administration of criminal justice and/or having law enforcement responsibilities.
- B. Data stored in the NCIC computer will include personal identification data, as well as public record data concerning each of the individual's major steps through the criminal justice process. A record concerning an individual will be initiated upon the first arrest of that individual for an offense meeting the criteria established for the national file. Each arrest will initiate a cycle in the record, which cycle will be complete upon the offender's discharge from the criminal justice process in disposition of that arrest.

- C. Each cycle in an individual's record will be based upon fingerprint identification. Ultimately the criminal fingerprint card documenting this identification will be stored at the state level or, in the case of a Federal offense, at the national level. At least one criminal fingerprint card must be in the files of the FBI Identification Division to support the computerized criminal history record in the index.
- D. The data, with respect to current arrests entered in the national index, will be restricted to serious and/or significant violations. Excluded from the national index will be juvenile offenders as defined by state law (unless the juvenile is tried in court as an adult); charges of drunkenness and/or vagrancy; certain public order offenses, i.e., disturbing the peace, curfew violations, loitering, false fire alarm; traffic violations (except data will be stored on arrests for manslaughter, driving under the influence of drugs or liquor, and "hit and run"); and nonspecific charges of suspicion or investigation.
- E. Data included in the system must be limited to that with the characteristics of public record, i.e.,
 - 1. Recorded by officers of public agencies or divisions thereof directly and principally concerned with crime prevention, apprehension, adjudication, or rehabilitation of offenders.
 - 2. The recording must have been made in satisfaction of public duty.
 - 3. The public duty must have been directly relevant to criminal justice responsibilities of the agency.
- F. Social history data should not be contained in the interstate criminal history system, e.g., narcotic civil commitment or mental hygiene commitment. If, however, such commitments are part of the criminal justice process, then they should be part of the system. Criminal history records and other law enforcement operational files should not be an integral part of a central data base containing noncriminal justice related information, e.g., welfare, hospital, education, revenue, and other such noncriminal files necessary for an orderly process in a democratic society.
- G. Each SCTA shall follow the law or practice of the state or, in the case of a Federal control terminal, the applicable Federal statute, with respect to purging/expunging data entered by the agency in the

nationally stored data. Data may be purged or expunged only by the agency originally entering that data. If the offender's entire record stored at the national level originates with one control terminal and all cycles are purged/expunged by that agency, all information, including personal identification data will be removed from the computerized NCIC file.

II. Steps to Assure Accuracy of Stored Information

- A. The FBI NCIC and SCTAs will make continuous checks on records being entered in the system to assure system standards and criteria are being met.
- B. Control terminal agencies shall adopt a careful and permanent program of data verification including:
 - 1. Systematic audits conducted to ensure that files have been regularly and accurately updated.
 - 2. Where errors or points of incompleteness are detected, the control terminal shall take immediate action to correct or complete the NCIC record as well as its own state record.

III. Who May Access Criminal History Data

- A. Direct access, meaning the ability to access the NCIC computerized file, will be permitted only under the management control of criminal justice agencies in the discharge of their official, mandated responsibilities. Agencies that will be permitted direct access to NCIC criminal history data include:
 - 1. Police forces and departments at all governmental levels that are responsible for enforcement of general criminal laws. This should be understood to include highway patrols and similar agencies.
 - 2. Prosecutive agencies and departments at all governmental levels.
 - 3. Courts at all governmental levels with a criminal or equivalent jurisdiction.
 - 4. Correction departments at all government levels, including corrective institutions and probation departments.
 - 5. Parole commissions and agencies at all governmental levels.

6. Agencies at all governmental levels which have as a principal function the collection and provision of fingerprint identification information.
7. State control terminal agencies which have as a sole function by statute the development and operation of a criminal justice information system.
8. Regional or local governmental organizations established pursuant to statute which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

IV. Control of Criminal Justice Systems

All computers, electronic switches, and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history information must be under the management control of criminal justice agencies. Similarly, satellite computers and manual terminals accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency. Management control is defined as the authority to set and enforce (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operation of computers, circuits and telecommunications terminals used to process criminal history record information insofar as the equipment is used to process, store, or transmit criminal history record information. Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the computerized criminal history program. Such management control guarantees the priority service needed by the criminal justice community. A criminal justice agency must have a written agreement with the noncriminal justice agency operating the data center assuring that the criminal justice agency has management control as defined above.

The Board continues to endorse the following statement by the Director of the FBI before the Subcommittee on Constitutional Rights on March 17, 1971: "If law enforcement or other criminal justice agencies are to be responsible for the confidentiality of the information in computerized systems, then they must have complete

management control of the hardware and the people who use and operate the system. These information systems should be limited to the function of serving the criminal justice community at all levels of government--local, state and Federal."

Although dedication is not required for NCIC CCH participation, the security of the information contained in a criminal record system and the priority service needed by the criminal justice community will be enhanced by compliance with the following concepts:

1. Success of law enforcement/criminal justice depends first on its manpower, adequacy and quality, and second on information properly processed, retrievable when needed, and used for decision making. Law enforcement can no more give up control of its information than it can its manpower.
2. Computerized information systems are made up of a number of integral parts, namely, the users, the operating staff, computers and related hardware, communications and terminal devices. For effectiveness, management control of the entire system cannot be divided. Likewise, the long-standing law enforcement fingerprint identification process is an essential element in the criminal justice system.
3. Traditionally, law enforcement/criminal justice has been responsible for the confidentiality of its information. This responsibility cannot be assumed if its data base is in a computer system out of law enforcement/criminal justice control.
4. The function of public safety and criminal justice demands the highest order of priority, 24 hours a day. Experience has shown that this priority is best achieved and maintained through dedicated systems.
5. A national/statewide public safety and criminal justice computer/communications system, because of priority, scope including system discipline, and information needs, on and off line, will require full service of hardware and operating personnel.
6. Traditionally, police and criminal justice information has not been intermingled or centrally stored with noncriminal social files such as revenue, welfare, and medical, etc. This concept is even more valid with respect to computerized information systems at both national and state levels.

7. These systems, particularly public safety and criminal justice information systems, must be functional and user oriented if they are to develop effectively. Computer skills are a part of the system. Ineffective systems result not only in the greatest dollar loss but also costs in lives.

V. Use of System-Derived Criminal History Data

- A. Criminal history data on an individual from the national computerized file will be made available to Federal agencies authorized under Executive Order or Federal statute and to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing or local or state employment, other than with a criminal justice agency, or for other uses unless such dissemination is pursuant to Federal or state statutes. Such state laws may not conflict with Federal law. There are no exceptions.
- B. Should any information be verified that any agency has received criminal history information and has disclosed that information to an unauthorized source, immediate action will be taken by NCIC to discontinue criminal history service to that agency, through the control terminal if appropriate, until the situation is corrected.
- C. Agencies should be instructed that their rights to direct access encompass only requests reasonably connected with their criminal justice responsibilities.
- D. The FBI NCIC and control terminals will make checks, as necessary, concerning inquiries made of the system to detect possible misuse.
- E. The establishing of adequate state and Federal criminal penalties for misuse of criminal history data is endorsed.
- F. Detailed computerized criminal history printouts shall contain caveats to the effect, "This response based on numeric identifier only" and "Official use only - arrest data based on fingerprints identification by submitting agency or FBI." These caveats will be generated by the FBI NCIC or state control terminal's computer or may be preprinted on paper stock.

VI. Right to Challenge Record

The person's right to see and challenge the contents of his/her record shall form an integral part of the system with reasonable administrative procedures.

If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC Interstate Identification Index (III), it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and Federal administrative and statutory regulation.

Appropriate identification includes being fingerprinted for the purpose of ensuring that he/she is the individual that he/she purports to be. The record on file will then be verified as his/her's through comparison of fingerprints.

The remote accessing of III for individual access and review is not allowed since states desire to follow individual state dissemination procedures for this purpose. The subject of the record indexed in III may submit a written request directly to: Federal Bureau of Investigation, NCIC Section, Washington, D.C., 20535, to obtain information concerning his or her record. The request must be accompanied by a set of rolled-inked fingerprint impressions, name, and date and place of birth. The NCIC will provide a copy of the Index record and Federal Offender File (FOF) record, if such exists. If the record is indexed for a participating state(s), NCIC will provide the name and address of the appropriate state agency(s) to contact.

Should an individual desire to challenge the accuracy or completeness of any of the information received from the FBI, he/she may direct application for correction or updating to the agency which contributed the questioned information or to the Director of the FBI. The FBI will forward the challenge to the agency which submitted the data requesting that the agency verify or correct the challenged entry. Upon receipt of official communication from the agency which contributed the original information, the FBI will make any necessary changes to the identification record and FOF record in accordance with the information supplied by that agency.

VII. Physical, Technical, and Personnel Security Measures

The following security measures are the minimum to be adopted by all agencies having access to the NCIC III. These measures are designed to prevent unauthorized access to the system data and/or unauthorized use of data obtained from the computerized file.

A. Computer Centers

1. The computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.
2. Since personnel at these computer centers can access data stored in the system, they must be screened thoroughly under the authority and supervision of an NCIC Control Terminal Agency (CTA). (This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a State Control Terminal Agency.) This screening will also apply to noncriminal justice maintenance or technical personnel.
3. All visitors to these computer centers must be accompanied by staff personnel at all times.
4. Computers having access to the NCIC must have the proper computer instructions written and other built-in controls to prevent criminal history data from being accessible to any terminals other than authorized terminals.
5. Computers having access to the NCIC must maintain a log of all transactions against the criminal history file. The NCIC identifies each specific agency entering or receiving information and maintains a complete record of those transactions. These transaction records and logs are in existence for review to detect possible misuse of criminal history data.
6. Each State Control Terminal Agency (SCTA) shall build its data system around a central computer, through which each inquiry must pass for screening and verification. The configuration and operation of the center shall provide for the integrity of the data base.

B. Communications

1. The circuit is a communications link between two or more points utilized by authorized agencies to transmit and receive information on behalf of criminal justice agencies.

2. Any agency that transmits data intra state over a communications circuit which is also used to transmit or receive criminal history information must be either a criminal justice agency or a noncriminal justice agency under the management control of a criminal justice agency, unless the NCIC CTA ensures that NCIC standards of service are met and the CTA has in place the necessary hardware and software protection to prevent the unauthorized or inadvertent dissemination of criminal history record information.
3. Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the transmission of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. When an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public, then details of criminal history record information may be transmitted.

C. Terminal Devices Having Access to NCIC

1. All agencies having terminals on the system must be required to physically place these terminals in secure locations within the authorized agency.
2. The agencies having terminals with access to criminal history must have terminal operators screened and restrict access to the terminal to a minimum number of authorized employees.
3. Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data.
4. The SCTA shall define procedures to ensure all metro computers and all remote terminals accessing the NCIC III File through the state system will maintain a manual or automated log of III inquiries with notation of the individual making request for the record. Metro systems accessing NCIC directly shall define procedures to ensure all remote terminals accessing the NCIC III File through such metro systems will maintain a manual or automated log of III inquiries with a notation of the individual making the request for the record, or

the metro systems may elect to maintain for any remote terminal an automated log of III inquiries with a notation of the individual making the request for the record. Manual terminals with a direct line to the NCIC, Washington, D.C., shall maintain a log of III inquiries with a notation of the individual making the request for the record. All NCIC III inquiry logs will be maintained for a minimum of one year.

A remote terminal is defined as a terminal accessing NCIC III through a state computer or through a metro computer which is either tied to a state computer or accesses NCIC directly.

VIII. The Role of the NCIC Advisory Policy Board Regarding Security and Confidentiality Matters

Periodically the NCIC Advisory Policy Board will consider and study the following areas:

- A. The consideration of criteria for the purging of records, i.e., deletion of records after a designated period of criminal inactivity or attainment of a specified age, etc.
- B. The consideration of criteria for qualification of noncriminal justice agencies for secondary access to criminal history data.
- C. A model state statute for protecting and controlling data in any future system should be drafted and its adoption encouraged.

IX. Organization and Administration

- A. Each CTA shall sign a written agreement with the NCIC to conform with system policy before participation in the criminal history program is permitted. This would allow for control over the data and give assurance of system security.
- B. In each state, the CTA shall prepare and execute a written agreement containing similar provisions to the agreement by the states and NCIC with each criminal justice agency having a terminal device capable of accessing criminal history data within that state.
- C. Each state criminal justice control terminal agency is responsible for the security throughout the system being serviced by that agency, including all places where terminal devices are located.

- D. A system security officer shall be designated in each CTA to assure all necessary physical, personnel, computer, and communications safeguards prescribed by the Advisory Policy Board are functioning properly in systems operations.
- E. The rules and procedures governing direct terminal access to criminal history data shall apply equally to all participants to the system, including the Federal and state control terminal agencies, and criminal justice agencies having access to the data stored in the system.
- F. All CTAs and other criminal justice agencies having direct access to computerized criminal history data from the system shall permit an inspection team appointed by the NCIC Advisory Policy Board to conduct appropriate inquiries with regard to any allegations of security violations. The inspection team shall include at least one representative of the FBI NCIC. All results of the investigation conducted shall be reported to the Advisory Policy Board with appropriate recommendations.
- G. Any noncompliance with these measures shall be brought to the immediate attention of the NCIC Advisory Policy Board. This Board has the responsibility for recommending action, including the discontinuing of service to enforce compliance with system security regulations.



U.S. Department of Justice
Federal Bureau of Investigation
National Crime Information Center (NCIC)

Bylaws for the NCIC Advisory Policy Board and Regional Working Groups

*Approved by NCIC Advisory Policy Board
October 17, 1984*

SMC-HD #6

For Official Use

BYLAWS FOR THE
NATIONAL CRIME INFORMATION CENTER
ADVISORY POLICY BOARD
AND REGIONAL WORKING GROUPS

Approved by NCIC
Advisory Policy Board
October 17, 1984

TABLE OF CONTENTS

		<u>PAGE</u>
1.0	<u>DEFINITIONS</u>	1
1.1	NCIC	1
1.2	NCIC REGIONAL WORKING GROUPS (RWG)	1
1.3	NCIC ADVISORY POLICY BOARD	2
1.4	CONTROL TERMINAL AGENCY (CTA)	3
1.5	SERVICE COORDINATOR AGENCY (SCA)	3
1.6	CONTROL TERMINAL OFFICER (CTO) AND SERVICE COORDINATOR (SC)	3
1.7	REGIONAL WORKING GROUP MEETINGS	3
1.8	PARTICIPANTS MEETINGS	4
1.9	DESIGNATED FEDERAL EMPLOYEE (DFE)	4
1.10	NCIC OPERATING MANUAL	4
1.11	MAIL BALLOTING	4
2.0	<u>ESTABLISHMENT OF BOARD</u>	4
3.0	<u>APPOINTED AND AT-LARGE MEMBERS</u>	5
3.1	TERM	5
4.0	<u>ELECTED MEMBERS OF THE BOARD</u>	5
4.1	NOMINATIONS	5
4.1.01	STATE REPRESENTATIVE	6
4.1.02	LOCAL REPRESENTATIVE	6
4.2	LIST OF CANDIDATES	6
4.3	VOTING	6
4.4	ELECTION	6
4.5	NOTIFICATION OF ELECTION	6
4.6	TERM	7
5.0	<u>VACANCIES ON THE BOARD</u>	7
5.1	PREVIOUS ELECTION	7
5.2	SPECIAL ELECTION	7
5.2.01	NOMINATIONS	7
5.2.02	VOTING AND ELECTION	8
6.0	<u>OFFICERS OF THE BOARD</u>	8
6.1	DUTIES OF OFFICERS	8
6.1.01	CHAIRMAN	8
6.1.02	VICE-CHAIRMEN	8
6.2	QUALIFICATION OF CHAIRMAN	8
6.3	NOMINATION OF CHAIRMAN	8
6.4	LIST OF CANDIDATES	9

TABLE OF CONTENTS (continued)

6.0	<u>OFFICERS OF THE BOARD</u> (continued)	
6.5	VOTING	9
6.6	ELECTION	9
6.7	NOTIFICATION OF DESIGNATED FEDERAL EMPLOYEE (DFE)	9
6.8	BALLOTING	9
6.9	TERM OF OFFICERS	10
6.10	VACANCY IN OFFICE OF CHAIRMAN	10
7.0	<u>MEETINGS</u>	10
7.1	TIME OF MEETINGS	10
7.2	PRESENCE OF DFE	10
7.3	COMPLIANCE WITH LAWS	10
7.4	NOTICE OF MEETINGS	10
7.5	CONDUCT OF MEETINGS	11
7.6	ATTENDANCE AT MEETINGS	11
7.7	OPEN SESSIONS	11
7.8	QUORUM	11
7.9	PROXIES	11
7.10	VOTING	12
7.11	RECONSIDERATION OF PAST ACTIONS	12
7.12	AGENDA	12
7.13	MINUTES OF MEETINGS	12
7.14	PUBLIC PARTICIPATION	13
	7.14.01 WRITTEN STATEMENTS	13
	7.14.02 ADDRESSING BOARD	13
	7.14.03 INFORMATION REQUIRED	13
	7.14.04 NOTIFICATION	13
	7.14.05 TIME LIMIT	13
7.15	VENDORS	14
7.16	ADJOURNMENT OF MEETINGS	14
8.0	<u>RECORDS OF BOARD</u>	14
9.0	<u>COMPENSATION OF BOARD MEMBERS</u>	14
10.0	<u>SUBCOMMITTEES</u>	14
11.0	<u>REGIONAL WORKING GROUPS (RWG)</u>	14
11.1	RWG OFFICERS	15
	11.1.01 QUALIFICATIONS	15
	11.1.02 NOMINATION AND ELECTION OF OFFICERS	15
	11.1.03 TERM OF OFFICE	15
	11.1.04 LIMITED TERMS	15
	11.1.05 DUTIES OF RWG CHAIRMEN	15
	11.1.06 VACANCIES IN RWG OFFICES	16

TABLE OF CONTENTS (continued)

11.0	<u>REGIONAL WORKING GROUPS (RWG)</u>	(continued)	
11.2	LOCAL RWG REPRESENTATIVES		16
	11.2.01 QUALIFICATIONS		17
	11.2.02 NOMINATIONS		17
	11.2.03 VOTING		17
	11.2.04 ELECTION		17
	11.2.05 TERM OF OFFICE		17
	11.2.06 TIME OF ELECTION		18
	11.2.07 LIMITATIONS		18
	11.2.08 RECORDS OF ELECTION		18
	11.2.09 ATTENDANCE AT RWG MEETINGS		18
	11.2.10 VACANCY OF LOCAL REPRESENTATIVE		19
	11.2.11 NOTIFICATION		19
11.3	RWG MEETINGS		20
	11.3.01 APPROVAL REQUIRED		20
	11.3.02 PUBLIC ATTENDANCE		20
	11.3.03 FEDERAL AGENCY SERVICE COORDINATOR		20
12.0	<u>DISCRIMINATION PROHIBITED</u>		20
13.0	<u>AMENDMENTS TO BYLAWS</u>		20

APPENDIX A

Federal Advisory Committee Act
(Public Law 92-463)

APPENDIX B

NCIC Charter

1.0 DEFINITIONS

1.1 NCIC

NCIC is the acronym for National Crime Information Center created pursuant to 28 U.S.C. 534. It is a computerized information center operated by the Federal Bureau of Investigation (FBI) for the benefit of Federal, state, and local criminal justice agencies. The files and systems contain but are not necessarily limited to:

- (1) Persons wanted for serious criminal offenses.
- (2) Missing persons.
- (3) Unidentified persons.
- (4) Stolen vehicles and vehicle parts and felony vehicles.
- (5) Stolen license plates.
- (6) Stolen boats.
- (7) Stolen securities.
- (8) Stolen articles.
- (9) Stolen and recovered guns.
- (10) Interstate Identification Index (III).
- (11) U.S. Secret Service Protective.

1.2 NCIC REGIONAL WORKING GROUPS (RWG)

To implement policy and procedures established for the NCIC, four Regional Working Groups are established

1.2 NCIC REGIONAL WORKING GROUPS (RWG) (continued)

throughout the United States. These Regional Working Groups are as follows:

North Central:	Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, Wisconsin
Northeastern:	Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont
Southern:	Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, Commonwealth of Puerto Rico, South Carolina, Tennessee, Virginia, West Virginia
Western:	Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Texas, Utah, Washington, Wyoming

The Regional Working Groups, through their respective Chairmen, will review operational issues of the NCIC System and make appropriate recommendations to the NCIC Advisory Policy Board or to the Designated Federal Employee.

1.3 NCIC ADVISORY POLICY BOARD

The NCIC Advisory Policy Board is composed of thirty representatives of criminal justice agencies throughout the United States. The Board will review issues related to the NCIC System and make appropriate recommendations to the Director of the FBI.

1.4 CONTROL TERMINAL AGENCY (CTA)

A CTA is a state or territorial criminal justice agency on the NCIC System providing statewide (or equivalent) service to its criminal justice users with respect to NCIC data. Only those agencies with direct telecommunications lines to NCIC may be control terminal agencies, and are held responsible for records entered through those lines. There will be no more than one CTA per state or territory.

1.5 SERVICE COORDINATOR AGENCY (SCA)

An NCIC SCA is a non-CTA which has a direct NCIC telecommunications line(s), which line will be used only for system query functions

1.6 CONTROL TERMINAL OFFICER (CTO) AND SERVICE COORDINATOR (SC)

An NCIC CTO and SC shall be appointed by the head of their respective agency.

The CTO/SC and his/her agency will be responsible for monitoring system use, enforcing system discipline, and assuring that NCIC operating procedures are followed by all users of the respective NCIC telecommunications lines as well as other related duties outlined by the NCIC User Agreement. When a new CTO or SC is designated, the CTA held will notify NCIC of that appointment within 10 days.

1.7 REGIONAL WORKING GROUP MEETINGS

Regional Working Groups will meet from time to time to consider NCIC policy and operational issues.

1.8 PARTICIPANTS MEETINGS

All Regional Working Group representatives will collectively meet as needed. Such meetings will also constitute a regional meeting to inform NCIC participants of the current status of the NCIC program and seek users' views on the various NCIC issues.

1.9 DESIGNATED FEDERAL EMPLOYEE (DFE)

The Director of the FBI will appoint a member of the Bureau to oversee the operations of the NCIC and to improve the scheduling of Regional Working Group and Board Meetings. This appointed member will be known as the Designated Federal Employee (DFE).

1.10 NCIC OPERATING MANUAL

An NCIC Operating Manual shall be maintained containing the procedures and codes necessary for the day-to-day operations of the NCIC network. It shall be provided on an as needed basis to NCIC users.

1.11 MAIL BALLOTING

Mail Balloting is a system by which the ballots are enclosed in a plain envelope and the plain envelope is enclosed in an outer addressed envelope.

2.0 ESTABLISHMENT OF BOARD

The NCIC Advisory Policy Board, composed of twenty elected members, six appointed members, and four at-large members, is created pursuant to the Federal Advisory Committee Act, 86 Stat. 770.

3.0 APPOINTED AND AT-LARGE MEMBERS

The Director of the FBI will appoint six members to the Advisory Policy Board as follows:

- (1) Two members from the judicial sector.
- (2) Two members from the prosecutorial sector.
- (3) Two members from the correctional sector.

One executive-level representative from each of the following professional criminal justice associations shall be designated by the respective association:

- (1) American Probation and Parole Association
- (2) International Association of Chiefs of Police
- (3) National District Attorneys Conference
- (4) National Sheriff's Association

3.1 TERM

The six FBI Director-appointed members shall each serve two-year terms and will be eligible for reappointment. The four professional criminal justice associations at-large member designations will be for two-year terms, subject to reappointment.

4.0 ELECTED MEMBERS OF THE BOARD

Elections of Board members shall be conducted by mail ballots by each RWG Chairman in August of each even-numbered year.

4.1 NOMINATIONS

Each State Control Terminal Agency may nominate candidates for membership on the NCIC Advisory Policy Board as follows:

4.1 NOMINATIONS (continued)

4.1.01 One executive level state criminal justice administrator.

4.1.02 One executive level local criminal justice administrator.

4.2 LIST OF CANDIDATES

Each Regional Chairman will prepare a list of nominees and furnish the list to the State Control Terminal Officers and elected local agency representatives within his/her region.

4.3 VOTING

Each elected local representative and each State Control Terminal Agency representative shall vote for four state representatives and one local representative within their respective region. Each ballot cast shall be signed by the voting party.

4.4 ELECTION

The four state level and the one local representative receiving the highest number of votes shall be elected to the Board from that region.

4.5 NOTIFICATION OF ELECTION

By September 5th following the election, the RWG Chairmen must advise the DFE of the results of the election and provide to him/her ballots cast for certification. Thereafter, ballots will be returned to the RWG Chairman and he/she will send the results to all members of the region.

4.6 TERM

Elected members shall serve a two-year term commencing December 12th following their election.

5.0 VACANCIES ON THE BOARD

A vacancy of an FBI Director-appointed member shall be filled by appointment by the Director of the FBI. A vacancy of a member from one of the four professional criminal justice associations shall be filled by appointment by the president of the respective association. A vacancy of an elected member will be filled by appointment of the respective Regional Chairman as follows:

5.1 PREVIOUS ELECTION

The RWG Chairman shall appoint the individual, state or local, depending on the vacancy, receiving the next highest vote total in the previous election to fill the unexpired term.

5.2 SPECIAL ELECTION

If the individual receiving the next highest vote in the previous election does not desire or is not available to serve, the Regional Chairman shall conduct a special election to fill the vacancy for the unexpired term.

5.2.01 NOMINATIONS

Nominations shall be made in the same manner as stated in Sections 4.1 and 4.2 of these Bylaws except that a nomination will not be made for a state level representative from any state which has a state representative on the Board.

5.2.02 VOTING AND ELECTION

The voting and election to fill a vacancy will be conducted as specified in Sections 4.3 and 4.4 of these Bylaws.

6.0 OFFICERS OF THE BOARD

The officers of the NCIC Board shall be a Chairman, First Vice-Chairman, Second Vice-Chairman, and Third Vice-Chairman.

6.1 DUTIES OF OFFICERS

6.1.01 Chairman - The Chairman shall be the presiding officer at each meeting of the NCIC Advisory Policy Board. The Chairman shall have sufficient authority, in consultation with the Vice-Chairmen, to act as spokesman for the criminal justice community in matters of a substantive dynamic nature affecting NCIC.

6.1.02 Vice-Chairmen - The First, Second and Third Vice-Chairmen shall act in the order of their election in the absence of the Chairman.

6.2 QUALIFICATION OF CHAIRMAN

The Chairman of the Board must be one of the twenty elected members of the NCIC Board.

6.3 NOMINATION OF CHAIRMAN

After the biennial election of Board members, each RWG Chairman will conduct an election by mail to determine their nominee for the position of Chairman.

6.4 LIST OF CANDIDATES

Each RWG Chairman will telephonically poll all newly elected Board members in his/her region to determine availability to serve as Board Chairman. Each RWG Chairman will then prepare a list of candidates and furnish the list to State Control Terminal Officers and elected local agency representatives within his/her region.

6.5 VOTING

Each elected local representative and each State Control Terminal Agency representative shall vote for one of the listed candidates. Each ballot cast shall be signed by the voting party.

6.6 ELECTION

The candidate receiving the highest number of votes shall be elected as the regional nominee for Board Chairman.

6.7 NOTIFICATION OF DESIGNATED FEDERAL EMPLOYEE (DFE)

By October 10th following the biennial election of members of the Board, each RWG Chairman must advise the DFE of the nominee from his/her region and provide to him/her ballots cast for certification. Thereafter, ballots will be returned to the RWG Chairmen.

6.8 BALLOTING

The DFE shall conduct balloting for election of the Chairman by mail among the elected and appointed members. Ballots must be returned to the DFE by November 5th.

6.9 TERM OF OFFICERS

The term of the officers shall be two years commencing the 12th day of December following their election. An elected Chairman may not serve more than two terms consecutively.

6.10 VACANCY IN OFFICE OF CHAIRMAN

A vacancy in the office of the Chairman of the Board shall be filled by the First Vice-Chairman and each other Vice-Chairman shall ascend accordingly.

7.0 MEETINGS

7.1 TIME OF MEETINGS

NCIC Advisory Policy Board meetings shall be held at least twice during each calendar year. Meetings shall be called by the DFE after consultation with the Advisory Committee Management Officer of the FBI. All meetings shall be held at a reasonable time in a place reasonably accessible to the public.

7.2 PRESENCE OF DFE

All Board meetings shall be conducted in the presence of the DFE or his/her alternate.

7.3 COMPLIANCE WITH LAWS

Meetings of the Board shall be conducted in accordance with the provisions of the Federal Advisory Committee Act, 86 Stat. 770.

7.4 NOTICE OF MEETINGS

Timely notice of all meetings shall be published in the Federal Register.

7.5 CONDUCT OF MEETINGS

All meetings shall be conducted in compliance with Roberts Rules of Order (latest revision) except as otherwise provided in these Bylaws.

7.6 ATTENDANCE AT MEETINGS

Members of the Board should attend all meetings. If a member fails to attend two consecutive Board meetings, regardless of proxy representation, such elected or appointed member shall automatically relinquish membership on the Board. Notification of such loss of membership shall be made by the Board Chairman to the member and his/her RWG Chairman or the Director of the FBI, if an appointed member.

7.7 OPEN SESSIONS

All meetings of the Board shall be conducted in open session unless determined otherwise by the DFE.

7.8 QUORUM

A quorum of the Board shall consist of sixteen members of the Board which may include proxies. No meeting will be held and no vote taken without a quorum being present.

7.9 PROXIES

A member sending a proxy must notify the Chairman of the Board in writing prior to the opening of the meeting for which the proxy is given. The proxy must be from the same criminal justice agency as the individual represented.

7.10 VOTING

Only members of the NCIC Advisory Policy Board or their proxies in attendance at the meeting shall be eligible to vote. Except for Bylaw amendments, all votes shall be decided by a simple majority of those members of the Board present.

7.11 RECONSIDERATION OF PAST ACTIONS

An action previously voted upon at any Board meeting and adopted may be reconsidered at the next duly constituted meeting if a person who voted in the direction of the motion moves to have the past action reconsidered.

7.12 AGENDA

The agenda for a meeting shall be set and mailed to each member at least twenty-one days prior to a meeting. A summary report of the RWG meetings will be placed on the agenda of the next regular meeting of the Board for its review.

Amendments to the agenda may be made up to the time of the meeting.

The Director of the FBI will be the final arbiter of all agenda items.

7.13 MINUTES OF MEETINGS

Minutes of meetings of the Board shall be kept and maintained by the DFE. Minutes of all meetings are available to the public upon request.

7.14 PUBLIC PARTICIPATION

7.14.01 WRITTEN STATEMENTS

Any member of the public shall be permitted to file a written statement with the Board before or after a meeting.

7.14.02 ADDRESSING BOARD

Any person who wishes to address a session of a meeting of the Board must notify the Advisory Committee Management Officer of the FBI, Washington, D.C. 20535, at least twenty-four hours prior to the commencement of the session.

7.14.03 INFORMATION REQUIRED

Name, corporate designation, consumer affiliation, or Government designation must be provided together with a capsulized version of the statement to be made and an outline of the material to be offered.

7.14.04 NOTIFICATION

Notification may be by mail, telegram, cable or hand-delivered note.

7.14.05 TIME LIMIT

A person will be allowed not more than fifteen minutes to cover his/her topic, except with the special approval of the Chairman of the Board.

7.15 VENDORS

Vendors will not be permitted to promote products or make sales presentations.

7.16 ADJOURNMENT OF MEETINGS

A meeting may be adjourned by the DFE if he feels it is in the public interest.

8.0 RECORDS OF BOARD

All records, transcripts, minutes and other documents relating to the advisory functions of the Board shall be administered by the FBI.

Records will be maintained in compliance with the Federal Advisory Committee Act.

9.0 COMPENSATION OF BOARD MEMBERS

Board members and subcommittee members shall receive no salary or other honorarium for their services.

Reimbursement for travel and subsistence expenses shall be made for attendance at meetings. Reimbursement shall be pursuant to 5 U.S.C. 5703.

10.0 SUBCOMMITTEES

The Chairman of the Board shall have the authority to create ad hoc subcommittees composed of Board members as needed.

11.0 REGIONAL WORKING GROUPS (RWG)

Four Regional Working Groups, consisting of one appointed State Control Terminal Agency representative for each state within the region and six elected local law enforcement representatives from within the region, are established by the DFE with the approval of the Director of the FBI.

11.1 REGIONAL WORKING GROUP OFFICERS

Each region will have a Chairman, First Vice-Chairman, and Second Vice-Chairman.

11.1.01 QUALIFICATIONS

Only officially appointed State Control Terminal Officers and elected local representatives to the region can be elected as officers. A member of the NCIC Advisory Policy Board cannot hold the office of Chairman of a Regional Working Group.

11.1.02 NOMINATION AND ELECTION OF OFFICERS

Nominations and elections will be held by secret ballot by July of even-numbered years to determine a Regional Chairman, First Vice-Chairman, and Second Vice-Chairman.

11.1.03 TERM OF OFFICE

The term of office for regional officers shall be from July of even-numbered years to the July of the next even-numbered year.

11.1.04 LIMITED TERMS

An elected Chairman may not serve more than three terms consecutively. This shall not constitute a ban to his holding other offices in the region.

11.1.05 DUTIES OF RWG CHAIRMEN

The Chairman of each RWG will:
. Preside over the RWG meetings.

11.1.05 DUTIES OF RWG CHAIRMEN (continued)

- . Forward to the FBI NCIC an up-to-date list of state and local representatives in his/her region within one month of taking office.
- . Conduct the election for local representatives and Board members.
- . Attend the Board meetings and present the views of his/her region.
- . Keep the RWG membership informed of NCIC matters.

11.1.06 VACANCIES IN RWG OFFICES

When there is a vacancy in the office of RWG Chairman he/she will be succeeded respectively by the First and Second Vice-Chairmen. In the event of a vacancy in the office of First Vice-Chairman, the Second Vice-Chairman shall succeed the First Vice-Chairman. If both offices become vacant, the Chairman of the RWG shall call for and hold an election for the remainder of the term of office by mail balloting.

If there is a vacancy in all offices of a RWG, the Chairman of the Board shall call for and hold an election in that region by mail balloting.

11.2 LOCAL RWG REPRESENTATIVES

In addition to the State Control Terminal representatives, six local law enforcement agencies shall be elected from within each RWG.

11.2.01 QUALIFICATIONS

Local representatives shall be management-level personnel from a law enforcement agency that maintains a telecommunications terminal or computer interface to the State Control Terminal Agency of NCIC.

11.2.02 NOMINATIONS

Only State Control Terminal Agencies shall nominate local law enforcement agencies. Only one local agency shall be accepted from a state and that nomination shall be confined to those agencies within their own state.

11.2.03 VOTING

All members of the RWG shall have the right to vote. Voting will be by mail ballot.

11.2.04 ELECTION

From the list of nominees, the voting membership must vote for three local agencies. The three nominees receiving the highest number of votes will be elected as agency representatives from the RWG.

11.2.05 TERM OF OFFICE

Terms of office for local law enforcement agencies shall be staggered, with three local agencies serving two-year terms from July 1 of even-numbered years and three local

11.2.05 TERM OF OFFICE (continued)

agencies serving two-year terms from July 1 of odd-numbered years. Local representatives may be elected to succeed themselves.

11.2.06 TIME OF ELECTION

Elections for the three local law enforcement agencies shall be held by July of each year.

11.2.07 LIMITATIONS

Not more than one local representative shall be elected from any one state within a region.

11.2.08 RECORDS OF ELECTION

The various Chairmen of the NCIC regions will maintain the records of elections and, if applicable, turn the results over to his successor.

11.2.09 ATTENDANCE AT RWG MEETINGS

Members of the Regional Working Groups should attend all meetings. If a State Control Terminal Agency fails to send a representative to a regional meeting, the RWG Chairman shall submit written notification of the failure to the involved agency. In the event a State Control Terminal Agency fails to send a representative to two consecutive meetings, the Chairman of the Advisory

11.2.09 ATTENDANCE AT RWG MEETINGS (continued)

Policy Board shall submit written notification of the failure to the Governor's Office of the involved state. In the event the elected local agency fails to send a representative to two consecutive regional meetings, such local agency shall automatically relinquish membership of the RWG, unless, in the event of a promotion, retirement, illness, or a transfer of the designated individual, the agency shall immediately notify the Regional Chairman and designate a replacement to represent the local agency.

11.2.10 VACANCY OF LOCAL REPRESENTATIVE

If a vacancy occurs at the local agency level, the RWG Chairman, after contacting the agency to verify willingness and desire to serve, shall appoint that agency receiving the next highest vote total in the election from which the vacancy occurs to fill the unexpired term.

11.2.11 NOTIFICATION

The RWG Chairman shall notify the DFE and the agency affected whenever a vacancy occurs.

11.3 RWG MEETINGS

11.3.01 APPROVAL REQUIRED

Each RWG Chairman must receive approval from the DFE prior to scheduling a regional meeting. A request for approval must be submitted in writing at least two months prior to the contemplated meeting.

11.3.02 PUBLIC ATTENDANCE

Public attendance at NCIC Participants, Regional, Technical and Ad Hoc Subcommittee Meetings, due to their nature and function, will be restricted to persons directly involved in NCIC matters.

11.3.03 FEDERAL AGENCY SERVICE COORDINATOR

Federal Agency Service Coordinators will generally attend Northeastern Regional Meetings at the Participants Meeting but are not authorized to vote on any issue.

12.0 DISCRIMINATION PROHIBITED

With regard to the election of Board and RWG members, there is to be no discrimination on the basis of race, color, national origin, religion, age, or sex.

13.0 AMENDMENTS TO BYLAWS

Proposed amendments must be mailed to the members of the Board at least twenty-one days before the meeting at which the amendment will be considered.

13.0 AMENDMENTS TO BYLAWS (continued)

These Bylaws may be amended by adoption of a motion. The motion must contain the exact wording of the change and contain an effective date. A two-thirds majority of the voting Board members present is required for the motion to pass.

APPENDIX A



Public Law 92-463
92nd Congress, H. R. 4383
October 6, 1972

An Act

86 STAT. 770

To authorize the establishment of a system governing the creation and operation of advisory committees in the executive branch of the Federal Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Advisory Committee Act".

Federal Advisory Committee Act.

FINDINGS AND PURPOSES

SEC. 2. (a) The Congress finds that there are numerous committees, boards, commissions, councils, and similar groups which have been established to advise officers and agencies in the executive branch of the Federal Government and that they are frequently a useful and beneficial means of furnishing expert advice, ideas, and diverse opinions to the Federal Government.

(b) The Congress further finds and declares that—

- (1) the need for many existing advisory committees has not been adequately reviewed;
- (2) new advisory committees should be established only when they are determined to be essential and their number should be kept to the minimum necessary;
- (3) advisory committees should be terminated when they are no longer carrying out the purposes for which they were established;
- (4) standards and uniform procedures should govern the establishment, operation, administration, and duration of advisory committees;
- (5) the Congress and the public should be kept informed with respect to the number, purpose, membership, activities, and cost of advisory committees; and
- (6) the function of advisory committees should be advisory only, and that all matters under their consideration should be determined, in accordance with law, by the official, agency, or officer involved.

DEFINITIONS

SEC. 3. For the purpose of this Act—

- (1) The term "Director" means the Director of the Office of Management and Budget.
- (2) The term "advisory committee" means any committee, board, commission, council, conference, panel, task force, or other similar group, or any subcommittee or other subgroup thereof (hereafter in this paragraph referred to as "committee"), which is—

- (A) established by statute or reorganization plan, or
 - (B) established or utilized by the President, or
 - (C) established or utilized by one or more agencies,
- in the interest of obtaining advice or recommendations for the President or one or more agencies or officers of the Federal Government, except that such term excludes (i) the Advisory Commission on Intergovernmental Relations, (ii) the Commission on Government Procurement, and (iii) any committee which is composed wholly of full-time officers or employees of the Federal Government.

(3) The term "agency" has the same meaning as in section 551(1) of title 5, United States Code.

(4) The term "Presidential advisory committee" means an advisory committee which advises the President.

APPLICABILITY

- Restrictions. SEC. 4. (a) The provisions of this Act or of any rule, order, or regulation promulgated under this Act shall apply to each advisory committee except to the extent that any Act of Congress establishing any such advisory committee specifically provides otherwise.
- (b) Nothing in this Act shall be construed to apply to any advisory committee established or utilized by—
- (1) the Central Intelligence Agency; or
 - (2) the Federal Reserve System.
- (c) Nothing in this Act shall be construed to apply to any local civic group whose primary function is that of rendering a public service with respect to a Federal program, or any State or local committee, council, board, commission, or similar group established to advise or make recommendations to State or local officials or agencies.

RESPONSIBILITIES OF CONGRESSIONAL COMMITTEES

- Review. SEC. 5. (a) In the exercise of its legislative review function, each standing committee of the Senate and the House of Representatives shall make a continuing review of the activities of each advisory committee under its jurisdiction to determine whether such advisory committee should be abolished or merged with any other advisory committee, whether the responsibilities of such advisory committee should be revised, and whether such advisory committee performs a necessary function not already being performed. Each such standing committee shall take appropriate action to obtain the enactment of legislation necessary to carry out the purpose of this subsection.
- Guidelines. (b) In considering legislation establishing, or authorizing the establishment of any advisory committee, each standing committee of the Senate and of the House of Representatives shall determine, and report such determination to the Senate or to the House of Representatives, as the case may be, whether the functions of the proposed advisory committee are being or could be performed by one or more agencies or by an advisory committee already in existence, or by enlarging the mandate of an existing advisory committee. Any such legislation shall—
- (1) contain a clearly defined purpose for the advisory committee;
 - (2) require the membership of the advisory committee to be fairly balanced in terms of the points of view represented and the functions to be performed by the advisory committee;
 - (3) contain appropriate provisions to assure that the advice and recommendations of the advisory committee will not be inappropriately influenced by the appointing authority or by any special interest, but will instead be the result of the advisory committee's independent judgment;
 - (4) contain provisions dealing with authorization of appropriations, the date for submission of reports (if any), the duration of the advisory committee, and the publication of reports and other materials, to the extent that the standing committee determines the provisions of section 10 of this Act to be inadequate; and

(b) contain provisions which will assure that the advisory committee will have adequate staff (either supplied by an agency or employed by it), will be provided adequate quarters, and will have funds available to meet its other necessary expenses.

(c) To the extent they are applicable, the guidelines set out in subsection (b) of this section shall be followed by the President, agency heads, or other Federal officials in creating an advisory committee.

RESPONSIBILITIES OF THE PRESIDENT

SEC. 6. (a) The President may delegate responsibility for evaluating and taking action, where appropriate, with respect to all public recommendations made to him by Presidential advisory committees.

(b) Within one year after a Presidential advisory committee has submitted a public report to the President, the President or his delegate shall make a report to the Congress stating either his proposals for action or his reasons for inaction, with respect to the recommendations contained in the public report.

Report to Congress.

(c) The President shall, not later than March 31 of each calendar year (after the year in which this Act is enacted), make an annual report to the Congress on the activities, status, and changes in the composition of advisory committees in existence during the preceding calendar year. The report shall contain the name of every advisory committee, the date of and authority for its creation, its termination date or the date it is to make a report, its functions, a reference to the reports it has submitted, a statement of whether it is an ad hoc or continuing body, the dates of its meetings, the names and occupations of its current members, and the total estimated annual cost to the United States to fund, service, supply, and maintain such committee. Such report shall include a list of those advisory committees abolished by the President, and in the case of advisory committees established by statute, a list of those advisory committees which the President recommends be abolished together with his reasons therefor. The President shall exclude from this report any information which, in his judgment, should be withheld for reasons of national security, and he shall include in such report a statement that such information is excluded.

Annual report to Congress.

Exclusion.

RESPONSIBILITIES OF THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET

SEC. 7. (a) The Director shall establish and maintain within the Office of Management and Budget a Committee Management Secretariat, which shall be responsible for all matters relating to advisory committees.

Committee Management Secretariat.

Establishment.

(b) The Director shall, immediately after the enactment of this Act, institute a comprehensive review of the activities and responsibilities of each advisory committee to determine—

Review.

(1) whether such committee is carrying out its purpose;

(2) whether, consistent with the provisions of applicable statutes, the responsibilities assigned to it should be revised;

(3) whether it should be merged with other advisory committees; or

(4) whether it should be abolished.

The Director may from time to time request such information as he deems necessary to carry out his functions under this subsection. Upon the completion of the Director's review he shall make recommendations to the President and to either the agency head or the Congress with respect to action he believes should be taken. Thereafter, the Director shall carry out a similar review annually. Agency heads shall cooperate with the Director in making the reviews required by this subsection.

Recommendations to President and Congress.

Agency cooperation.

Performance
guidelines.

(c) The Director shall prescribe administrative guidelines and management controls applicable to advisory committees, and, to the maximum extent feasible, provide advice, assistance, and guidance to advisory committees to improve their performance. In carrying out his functions under this subsection, the Director shall consider the recommendations of each agency head with respect to means of improving the performance of advisory committees whose duties are related to such agency.

Uniform pay
guidelines.

(d) (1) The Director, after study and consultation with the Civil Service Commission, shall establish guidelines with respect to uniform fair rates of pay for comparable services of members, staffs, and consultants of advisory committees in a manner which gives appropriate recognition to the responsibilities and qualifications required and other relevant factors. Such regulations shall provide that—

(A) no member of any advisory committee or of the staff of any advisory committee shall receive compensation at a rate in excess of the rate specified for GS-18 of the General Schedule under section 5332 of title 5, United States Code; and

Travel expenses.

(B) such members, while engaged in the performance of their duties away from their homes or regular places of business, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for persons employed intermittently in the Government service.

80 Stat. 499;
83 Stat. 190.

(2) Nothing in this subsection shall prevent—

(A) an individual who (without regard to his service with an advisory committee) is a full-time employee of the United States, or

(B) an individual who immediately before his service with an advisory committee was such an employee, from receiving compensation at the rate at which he otherwise would be compensated (or was compensated) as a full-time employee of the United States.

Expense recom-
mendations.

(e) The Director shall include in budget recommendations a summary of the amounts he deems necessary for the expenses of advisory committees, including the expenses for publication of reports where appropriate.

RESPONSIBILITIES OF AGENCY HEADS

SEC. 8. (a) Each agency head shall establish uniform administrative guidelines and management controls for advisory committees established by that agency, which shall be consistent with directives of the Director under section 7 and section 10. Each agency shall maintain systematic information on the nature, functions, and operations of each advisory committee within its jurisdiction.

Advisory Com-
mittee Manage-
ment Control
Officer, design-
ation.

(b) The head of each agency which has an advisory committee shall designate an Advisory Committee Management Officer who shall—

(1) exercise control and supervision over the establishment, procedures, and accomplishments of advisory committees established by that agency;

(2) assemble and maintain the reports, records, and other papers of any such committee during its existence; and

(3) carry out, on behalf of that agency, the provisions of section 552 of title 5, United States Code, with respect to such reports, records, and other papers.

81 Stat. 54.

ESTABLISHMENT AND PURPOSE OF ADVISORY COMMITTEES

SEC. 9. (a) No advisory committee shall be established unless such establishment is—

(1) specifically authorized by statute or by the President; or

(2) determined as a matter of formal record, by the head of the agency involved after consultation with the Director, with timely notice published in the Federal Register, to be in the public interest in connection with the performance of duties imposed on that agency by law.

Publication in
Federal Register.

(b) Unless otherwise specifically provided by statute or Presidential directive, advisory committees shall be utilized solely for advisory functions. Determinations of action to be taken and policy to be expressed with respect to matters upon which an advisory committee reports or makes recommendations shall be made solely by the President or an officer of the Federal Government.

(c) No advisory committee shall meet or take any action until an advisory committee charter has been filed with (1) the Director, in the case of Presidential advisory committees, or (2) with the head of the agency to whom any advisory committee reports and with the standing committees of the Senate and of the House of Representatives having legislative jurisdiction of such agency. Such charter shall contain the following information:

Charter,
filing.

Contents.

- (A) the committee's official designation;
- (B) the committee's objectives and the scope of its activity;
- (C) the period of time necessary for the committee to carry out its purposes;
- (D) the agency or official to whom the committee reports;
- (E) the agency responsible for providing the necessary support for the committee;
- (F) a description of the duties for which the committee is responsible, and, if such duties are not solely advisory, a specification of the authority for such functions;
- (G) the estimated annual operating costs in dollars and man-years for such committee;
- (H) the estimated number and frequency of committee meetings;
- (I) the committee's termination date, if less than two years from the date of the committee's establishment; and
- (J) the date the charter is filed.

A copy of any such charter shall also be furnished to the Library of Congress.

Copy.

ADVISORY COMMITTEE PROCEDURES

SEC. 10. (a) (1) Each advisory committee meeting shall be open to the public.

Meetings.

(2) Except when the President determines otherwise for reasons of national security, timely notice of each such meeting shall be published in the Federal Register, and the Director shall prescribe regulations to provide for other types of public notice to insure that all interested persons are notified of such meeting prior thereto.

Notice.
Publication in
Federal Register.
Regulations.

(3) Interested persons shall be permitted to attend, appear before, or file statements with any advisory committee, subject to such reasonable rules or regulations as the Director may prescribe.

(b) Subject to section 552 of title 5, United States Code, the records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by each advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist.

81 Stat. 54.

(c) Detailed minutes of each meeting of each advisory committee shall be kept and shall contain a record of the persons present, a complete and accurate description of matters discussed and conclusions reached, and copies of all reports received, issued, or approved by the

Minutes.

86 STAT. 775

Certification.

advisory committee. The accuracy of all minutes shall be certified to by the chairman of the advisory committee.

81 Stat. 54.

Annual report.

(d) Subsections (a) (1) and (a) (3) of this section shall not apply to any advisory committee meeting which the President, or the head of the agency to which the advisory committee reports, determines is concerned with matters listed in section 552 (b) of title 5, United States Code. Any such determination shall be in writing and shall contain the reasons for such determination. If such a determination is made, the advisory committee shall issue a report at least annually setting forth a summary of its activities and such related matters as would be informative to the public consistent with the policy of section 552 (b) of title 5, United States Code.

Federal officer
or employee,
attendance.

(e) There shall be designated an officer or employee of the Federal Government to chair or attend each meeting of each advisory committee. The officer or employee so designated is authorized, whenever he determines it to be in the public interest, to adjourn any such meeting. No advisory committee shall conduct any meeting in the absence of that officer or employee.

(f) Advisory committees shall not hold any meetings except at the call of, or with the advance approval of, a designated officer or employee of the Federal Government, and in the case of advisory committees (other than Presidential advisory committees), with an agenda approved by such officer or employee.

AVAILABILITY OF TRANSCRIPTS

SEC. 11. (a) Except where prohibited by contractual agreements entered into prior to the effective date of this Act, agencies and advisory committees shall make available to any person, at actual cost of duplication, copies of transcripts of agency proceedings or advisory committee meetings.

"Agency pro-
ceeding."
80 Stat. 382.

(b) As used in this section "agency proceeding" means any proceeding as defined in section 551 (12) of title 5, United States Code.

FISCAL AND ADMINISTRATIVE PROVISIONS

Recordkeeping.

Audit.

Agency sup-
port services.

SEC. 12. (a) Each agency shall keep records as will fully disclose the disposition of any funds which may be at the disposal of its advisory committees and the nature and extent of their activities. The General Services Administration, or such other agency as the President may designate, shall maintain financial records with respect to Presidential advisory committees. The Comptroller General of the United States, or any of his authorized representatives, shall have access, for the purpose of audit and examination, to any such records.

(b) Each agency shall be responsible for providing support services for each advisory committee established by or reporting to it unless the establishing authority provides otherwise. Where any such advisory committee reports to more than one agency, only one agency shall be responsible for support services at any one time. In the case of Presidential advisory committees, such services may be provided by the General Services Administration.

RESPONSIBILITIES OF LIBRARY OF CONGRESS

Reports and
background
papers.

Depository.

SEC. 13. Subject to section 552 of title 5, United States Code, the Director shall provide for the filing with the Library of Congress of at least eight copies of each report made by every advisory committee and, where appropriate, background papers prepared by consultants. The Librarian of Congress shall establish a depository for such reports and papers where they shall be available to public inspection and use.

TERMINATION OF ADVISORY COMMITTEES

SEC. 14. (a) (1) Each advisory committee which is in existence on the effective date of this Act shall terminate not later than the expiration of the two-year period following such effective date unless—

(A) in the case of an advisory committee established by the President or an officer of the Federal Government, such advisory committee is renewed by the President or that officer by appropriate action prior to the expiration of such two-year period; or

(B) in the case of an advisory committee established by an Act of Congress, its duration is otherwise provided for by law.

(2) Each advisory committee established after such effective date shall terminate not later than the expiration of the two-year period beginning on the date of its establishment unless—

(A) in the case of an advisory committee established by the President or an officer of the Federal Government such advisory committee is renewed by the President or such officer by appropriate action prior to the end of such period; or

(B) in the case of an advisory committee established by an Act of Congress, its duration is otherwise provided for by law.

(b) (1) Upon the renewal of any advisory committee, such advisory committee shall file a charter in accordance with section 9(c). Renewal.

(2) Any advisory committee established by an Act of Congress shall file a charter in accordance with such section upon the expiration of each successive two-year period following the date of enactment of the Act establishing such advisory committee.

(3) No advisory committee required under this subsection to file a charter shall take any action (other than preparation and filing of such charter) prior to the date on which such charter is filed.

(c) Any advisory committee which is renewed by the President or any officer of the Federal Government may be continued only for successive two-year periods by appropriate action taken by the President or such officer prior to the date on which such advisory committee would otherwise terminate. Continuation.

EFFECTIVE DATE

SEC. 15. Except as provided in section 7(b), this Act shall become effective upon the expiration of ninety days following the date of enactment.

Approved October 6, 1972.

LEGISLATIVE HISTORY:

HOUSE REPORTS: No. 92-1017 (Comm. on Government Operations) and No. 92-1403 (Comm. of Conference).

SENATE REPORT No. 92-1098 accompanying S. 3529 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 118 (1972):

May 9, considered and passed House.

Sept. 12, considered and passed Senate, amended, in lieu of S. 3529.

Sept. 19, Senate agreed to conference report.

Sept. 20, House agreed to conference report.

APPENDIX B

I. CHARTER - NCIC ADVISORY POLICY BOARD (Rev. 1/14/87)

A. Official Designation

This charter relates to the National Crime Information Center (NCIC) Advisory Policy Board, referred to herein as the Board.

B. The Board's Objectives and Scope of Activity

To recommend to the FBI general policy with respect to the philosophy, concept, and operational principles of the NCIC, particularly the system's relationships with local and state systems.

To review and consider rules, regulations, and procedures for the operation of NCIC.

To consider the NCIC operational needs of criminal justice agencies in the light of public policy and local, state, and Federal statutes.

To review and consider security and privacy aspects of the NCIC System.

To recommend standards for participation by criminal justice agencies in the NCIC System.

C. Duration of Tenure

The period of time necessary for the Board to carry out its purpose is indefinite.

This charter expires 2 years from its effective date, and is subject to renewal.

D. Reporting

The Board shall report to the Director of the FBI or his designated appointee.

E. Support Services

The FBI will provide all necessary support services for the Board.

F. Duties

The duties of the Board are advisory and are to carry out the objectives listed in item B.

The Chairman may appoint ad hoc committees as needed to assist the Board in its deliberations.

G. Annual Operating Costs

The estimated annual operating cost of the Board is expected to be \$348,000. These costs involve four and

G. Annual Operating Costs (continued)

one-half man-years of support services and expenses of Board members to attend meetings.

H. Meetings

The Board will meet at least twice each year at approximate six-month intervals. The Board meetings will be open to the public unless determined otherwise by the Designated Federal Employee.

I. Establishing Authority

The NCIC Advisory Policy Board was established by the Director of the FBI in February, 1969, to aid in the development of NCIC.

J. Termination Date

The Board's termination date is indefinite.

K. Date of Charter

January 14, 1987.

William H. Webster
Director

CONTROL TERMINAL OFFICER LIST

ALABAMA

CONTROL TERMINAL OFFICER

Mr. Pete Petrov AL003065Y
Criminal Justice Information Center
770 Washington Avenue
Montgomery, AL 36130
(205-242-4900)
FAX (205) 242-0577

OPERATIONAL (Quality Control, Validations, Etc.)

Mr. James H. Ingram AL003015Y
Alabama Criminal Justice Information Center
770 Washington Avenue
Montgomery, AL 36130
(205-242-4916)

III

Mr. Ron Cunningham AL003025Y
CCH Project Leader
770 Washington Avenue
Montgomery, AL 36130
(205-242-4913)

ALASKA

CONTROL TERMINAL OFFICER

Mr. Peter G. Davis AKAST0102
Supervisor of Records and Identification
Department of Public Safety
Information Systems Section
5700 East Tudor Road
Anchorage, AK 99507
(907-269-5708)
FAX (907) 269-5617

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

SMC-HD #7

1
5/13/92

200

ARIZONA

CONTROL TERMINAL OFFICER

Mr. Richard Carlson
Assistant Director of
Telecommunications
Arizona Department of Public Safety
P. O. Box 6638
Phoenix, AZ 85005-6638
(602-223-2404)
FAX (602) 223-2916

AZCCHPX00

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

ARKANSAS

CONTROL TERMINAL OFFICER

Mr. Charles Pruitt
Deputy Director
Arkansas Crime Information Center
One Capitol Mall, 4D-200
Little Rock, AR 72201
(501-682-2222)
FAX (501) 682-7444

AR060015Y

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

CALIFORNIA

CONTROL TERMINAL OFFICER

Mr. Fred H. Wynbrandt
Chief
Bureau of Criminal Information and Analysis
California Department of Justice
Post Office Box 903387
Sacramento, CA 94203-3870
(916-739-3936)
FAX (916) 739-5495

CA0349400

OPERATIONAL (Quality Control, Validations, Etc.)

Mr. Dave Miller
Manager, Command Communications
and Compliance Program
Post Office Box 13417
Sacramento, CA 95813
(916-739-5104)

CA0349400

III

Mr. Robert Siegle, Manager
CJIS Support Section
Law Enforcement Data Center
California Department of Justice
Post Office Box 903307
Sacramento, CA 94203
(916-739-2210)

CA0349400

COLORADO

CONTROL TERMINAL OFFICER

Mr. W. Gray Buckley
Inspector
Colorado Bureau of Investigation
690 Kipling Street, Suite 3000
Denver, CO 80215
(303-239-4224)
(303-239-4222--CCIC 24 hours)
FAX (303) 235-0568

COCBI0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Ms. Cecelia Franklin
Colorado Bureau of Investigation
690 Kipling Street, Suite 3000
Denver, CO 80215
(303-239-4235)

COCBI0001

CONNECTICUT

CONTROL TERMINAL OFFICER

Ms. Maryjane D'Aloia
Connecticut Online Law Enforcement
Communications and Teleprocessing
Department of State Police
294 Colony Street
Meriden, CT 06450
(203-238-6656)
FAX (203) 238-6447

CTCSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

DELAWARE

CONTROL TERMINAL OFFICER

Mr. Benjamin H. Miller
Chief, Communications Center
Delaware State Police Headquarters
Department of Public Safety
Post Office Box 430
Dover, DE 19903
(302-739-5851)
FAX (302) 736-1729

DEDSP00C7

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Ms. Sharon Emerson
State Bureau of Identification
Delaware State Police Headquarters
Post Office Box 430
Dover, DE 19901
(302-739-5977)

DEDSP0000

DISTRICT OF COLUMBIA

CONTROL TERMINAL OFFICER

Inspector David W. Bostrom
Director, Data Processing Division
Metropolitan Police Department
Room 1125
300 Indiana Avenue, Northwest
Washington, DC 20001
(202-727-4301)
FAX (202) 727-3896

DCMPD00M7

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

FLORIDA

203

4

5/13/92

CONTROL TERMINAL OFFICER

Mr. Patrick J. Doyle
Director
Division of Criminal Justice
Information Systems
Department of Law Enforcement
2331 Phillips Road
Tallahassee, FL 32308
(904-488-3961)
FAX (904) 487-1030

FL03701F3

OPERATIONAL (Quality Control, Validations, Etc.)

Mr. Ritchie Grant
Field Support Section
Division of Criminal Justice Information Systems
Florida Department of Law Enforcement
Post Office Box 1489
Tallahassee, FL 32302
(904-488-6041)

FL0370100

III

Mr. Rick Duggar
Systems and Programming Manager
Department of Law Enforcement
Post Office Box 1489
Tallahassee, FL 32302
(904-488-6041)

FL0370100

GEORGIA

CONTROL TERMINAL OFFICER

Mr. Thomas J. McGreevy
Deputy Director for GCIC
Georgia Bureau of Investigation
Post Office Box 370748
Decatur, GA 30037-0748
(404-244-2601)
FAX (404) 241-5992

GAGBI0091

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

HAWAII

CONTROL TERMINAL OFFICER

Major Barry Fujii
Research and Development Division
Honolulu Police Department
1455 South Beretania Street
Honolulu, HI 96814
(808-943-3121)
FAX (808) 943-3525

HI0020000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

IDAHO

CONTROL TERMINAL OFFICER

Mr. A. D. Jones
Chief
Idaho Bureau of
Criminal Identification
Idaho Department of Law Enforcement
6064 Corporal Lane
Boise, ID 83704
(208-327-7137)
FAX (208) 327-7138

ID001015Y

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

ILLINOIS

CONTROL TERMINAL OFFICER

Mr. Richard V. White
LEADS Administrator
Illinois State Police
P.O. Box 19461
301 Armory Building
Springfield, IL 62794-9461
(217-782-4038)
FAX (217) 782-4036

IL0849600

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. John Loverude
CCH Project Leader
Bureau of Identification
Illinois Department of State Police
260 N. Chicago Street
Joliet, IL 60431
(815-740-5160)

IL0998900

INDIANA

CONTROL TERMINAL OFFICER

Major Fred Pryor
Indiana State Police
Indiana Government Center North
Criminal Justice Data Division
100 North Senate Avenue, Room 113A
Indianapolis, IN 46204-2259
(317-232-8260)
FAX (317) 232-0652

INISP0007

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

IOWA

CONTROL TERMINAL OFFICER

Mr. Carroll L. Bidler
Administrator of Administrative
Services
Wallace State Office Building
Des Moines, IA 50319
(515-281-8422)
FAX (515) 242-6136

IADPS0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

IADPS0001

III

(Same as above)

KANSAS

CONTROL TERMINAL OFFICER

Major David L. Hornbaker
Kansas Highway Patrol
122 Southwest Seventh Street
Topeka, KS 66603
(913-296-6800)
FAX (913) 296-5956

KSKHPQ000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. David E. Johnson
Director
Kansas Bureau of Investigation
1620 Tyler
Topeka, KS 66612
(913-232-6000)

KSKBI0000

KENTUCKY

CONTROL TERMINAL OFFICER

Major Neal Brittain
Commander
Information Services Branch
Kentucky State Police
1250 Louisville Road
Frankfort, KY 40601
(502-227-8700)
FAX (502) 227-8734

KYKSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

LOUISIANA

CONTROL TERMINAL OFFICER

Mr. Bruce F. Wisner
Supervisor of Communications
Louisiana State Police
Department of Public Safety
Post Office Box 66614
Baton Rouge, LA 70896
(504-925-6325)
FAX (504) 925-4766

LALSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

MAINE

CONTROL TERMINAL OFFICER

Sergeant Walter R. Chapin, Jr.
Director of Communications
Maine State Police
36 Hospital Street
Augusta, ME 04330
(207-621-1283)
FAX (207) 289-2098

MEMSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

MARYLAND

CONTROL TERMINAL OFFICER

Second Lieutenant Thomas F. Murrill
Telecommunications Division
Maryland State Police Headquarters
Pikesville, MD 21208
(301-653-4356)
FAX (301) 653-4269

MDMSP0005

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

MASSACHUSETTS

CONTROL TERMINAL OFFICER

Mr. John P. Cloherty
Assistant Director
Executive Office of Public Safety
Criminal History Systems Board
1010 Commonwealth Avenue
Boston, MA 02215
(617-727-0090)
FAX (617) 232-1104

MAMSP0054

OPERATIONAL (Quality Control, Validations, Etc.)

Mr. Jim Slater
Quality Control Unit
1010 Commonwealth Avenue
Boston, MA 02115
(617-727-0090)

MAMSP0054

III

(Same as Control Terminal Officer)

MICHIGAN

CONTROL TERMINAL OFFICER

Mr. Jack Pooler
Executive Secretary
LEIN Policy Council
Michigan State Police
714 South Harrison Road
East Lansing, MI 48823
(517-336-6166)
FAX (517) 336-6256

MI3300203

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Ms. Marie Pifer
Michigan State Police
Central Records Division
7150 Harris Drive
Lansing, MI 48913
(517-322-5511)

MI3300800

MINNESOTA

CONTROL TERMINAL OFFICER

Mr. Kenneth A. Bentfield
Minnesota Department of Public Safety
Director, Office of Information
Systems Management
Room 314, Transportation Building
395 John Ireland Boulevard
St. Paul, MN 55155
(612-296-7589)
FAX (612) 297-5728

MNBCA0000

OPERATIONAL (Quality Control, Validations, Etc.)

Ms. Karen McDonald
Criminal Justice Information System
Minnesota Department of Public Safety - BCA
1246 University Avenue
St. Paul, MN 55104-4197

III

(Same as above)

MISSISSIPPI

CONTROL TERMINAL OFFICER

Mr. Will Spann
Director
Management Information Systems
Criminal Justice Information Center
Department of Public Safety
Post Office Box 958
Jackson, MS 39205
(601-987-1337)
FAX (601) 987-1480

MSMHP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

MISSOURI

CONTROL TERMINAL OFFICER

Dr. Robert J. Bradley
Director
Information Systems Division
Missouri State Highway Patrol
Department of Public Safety
Post Office Box 568
Jefferson City, MO 65102
(314-751-3313)
FAX (314) 751-9382

MOMHP0040

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Captain Bob Howard
Missouri State Highway Patrol
1510 East Elm Street
Jefferson City, MO 65101
(314-751-3313)

MOMHP0001

MONTANA

CONTROL TERMINAL OFFICER

Mr. John Mathews
Administrator
Data Processing Division
Montana Department of Justice
303 North Roberts
Helena, MT 59620
(406-444-2424 or 2800)
FAX (406) 444-4169

MT025015Y

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. Michael J. Miller
Bureau Chief
State Identification Bureau
Montana Department of Justice
303 North Roberts
Helena, MT 59620
(406-444-3625)

MT025025Y

NEBRASKA

CONTROL TERMINAL OFFICER

Lieutenant Ray R. Kastanek
Director of Communications
Nebraska State Patrol
Post Office Box 94907
State House Station
Lincoln, NE 68509-4907
(402-471-4545)
FAX (402) 479-4002

NBNSPOD00

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Ms. Marlene Dailey
Nebraska State Patrol
Post Office Box 94907
State House Station
Lincoln, NE 68509
(402-479-4924)

NBNSPOD00

NEVADA

CONTROL TERMINAL OFFICER

Mr. Dennis A. DeBacco
Manager
Criminal Information Services Section
Nevada Highway Patrol
555 Wright Way
Carson City, NV 89711
(702-687-5713)
FAX (702) 687-3693

NV0139900

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

NEW HAMPSHIRE

CONTROL TERMINAL OFFICER)

Major Frederick H. Booth
State Police Headquarters
Hazen Drive
Concord, NH 03305
(603-271-1020)
FAX (603) 271-1153

NHNSP0080

OPERATIONAL (Quality Control, Validations, Etc.)

Ms. Diane Auclair
NCIC Operations Officer
New Hampshire State Police
Concord, NH 03301

NHNSP0000

III

(Same as Control Terminal Officer)

NEW JERSEY

CONTROL TERMINAL OFFICER

SFC Wayne Zelenak
CJIS Control Unit
New Jersey State Police Headquarters
Box 7068
West Trenton, NJ 08628-0068
(609-882-2000, ext. 2294)
FAX (609) 882-6523

NJNSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Captain Jim Petrecca
State Bureau of Identification
Division of State Police
Post Office Box 7068
West Trenton, NJ 08625
(609-882-2000)

NJNSP0200

NEW MEXICO

CONTROL TERMINAL OFFICER

Major Don L. Helberg
Director
Technical and Emergency Support Division
Department of Public Safety
Post Office Box 1628
Santa Fe, NM 87504-1628
(505-827-3411)
FAX (505) 827-3396

NMNSP0026

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Ms. Irene I. Trujillo
Director, Records Division
New Mexico State Police
Post Office Box 1628
Santa Fe, NM 87501
(505-827-9181)

NMNSP0000

NEW YORK

CONTROL TERMINAL OFFICER

Mr. John B. Campbell
Director, Data Processing
New York State Police
State Campus, Building #22
Albany, NY 12226
(518-457-2393)
FAX (518) 457-3207

NY1010000

OPERATIONAL (Quality Control, Validations, Etc.)

Captain Andrew Chiasera
Director of Management Information Systems
New York City Police Department
1 Police Plaza - Room 700
New York, NY 10038
(212-374-5020)

NY0303000

III

Ms. Patricia Zabinski
New York State Division of Criminal
Justice Services
Executive Park Tower
Stuyvesant Plaza
Albany, NY 12203
(518-457-6066)

NY001015Y

NORTH CAROLINA

CONTROL TERMINAL OFFICER

Mr. William C. Corley
Assistant Director
Division of Criminal Information
State Bureau of Investigation
407 North Blount Street
Raleigh, NC 27601
(919-733-3171)
FAX (919) 733-8378

NCDCI0002

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

NORTH DAKOTA

CONTROL TERMINAL OFFICER

Mr. James D. Lueder
Assistant Director
North Dakota State Radio Communications
Post Office Box 5511
Bismarck, ND 58502-5511
(701-224-2127)
FAX (701) 224-2126

NDRCD0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. Richard S. Hilde
Superintendent
Bureau of Criminal Investigation
Post Office Box 1054
Bismarck, ND 58501
(701-221-6180)

NDBCA0000

OHIO

CONTROL TERMINAL OFFICER

Major Donald A. Mack
Commander
Office of Support Services
Ohio State Highway Patrol
Post Office Box 7037, Station E
Columbus, OH 43205-0037
(614-466-3554) or (614-466-5933)
FAX (614) 644-9749

OHOHP0099

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. Marlin Dowler
Identification Division Chief
Ohio Bureau of Criminal Identification
and Investigation
Post Office Box 365
State Route #56
London, OH 43140
(614-852-2556 or 2561)

OHBCI0000

OKLAHOMA

CONTROL TERMINAL OFFICER

Mr. Brad Long
Director
Oklahoma Law Enforcement
Telecommunications System
Post Office Box 11415
Oklahoma City, OK 73136
(405-425-2224)
FAX (405) 425-2029

OKOLETS00

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. Ron Young
Identification and Communications Administrator
Oklahoma State Bureau of Investigation
Post Office Box 11497
Oklahoma City, OK 73136
(405-427-5421)

OKOBI0000

OREGON

CONTROL TERMINAL OFFICER

Mr. Lloyd A. Smith
Manager
Oregon Law Enforcement Data System
155 Cottage Street, Northeast
Salem, OR 97310
(503-378-3054)
FAX (503) 363-8249

OR024015Y

OPERATIONAL (Quality Control, Validations, Etc.)

Mr. Paul Regimbal
Law Enforcement Data System
955 Center Street, Northeast
Salem, OR 97310
(503-378-3144)

III

(Same as above)

PENNSYLVANIA

CONTROL TERMINAL OFFICER

Lieutenant Michael R. Weir
Pennsylvania State Police
Department Headquarters
1800 Elmerton Avenue
Harrisburg, PA 17110
(717-787-1585)
FAX (717) 783-4384

PAPSP0007

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Captain Francis Panuccio
Pennsylvania State Police
Department Headquarters
1800 Elmerton Avenue
Harrisburg, PA 17110
(717-783-5592)

PAPSP0000

RHODE ISLAND

CONTROL TERMINAL OFFICER

Mr. Brian J. Glancy
Computer Services Section
Rhode Island State Police
Post Office Box 185
North Scituate, RI 02857
(401-647-3311)
FAX (401) 647-3014

RIRSP0006

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

SOUTH CAROLINA

CONTROL TERMINAL OFFICER

Captain James V. Martin
South Carolina Law Enforcement Division
Post Office Box 21398
Columbia, SC 29221
(803-737-9029)
FAX (803) 737-2967

SCLED0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

Mr. Steve Hanayik
Law Enforcement Division
Post Office Box 21398
Columbia, SC 29221
(803-737-8794)

SOUTH DAKOTA

CONTROL TERMINAL OFFICER

Mr. Delton Keith Tipton
Attorney General's Office
Criminal Justice Training Center
500 East Capitol Avenue
Pierre, SD 57501
(605-773-3536)
FAX (605) 773-4629

SDDCI0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

TENNESSEE

CONTROL TERMINAL OFFICER

Mr. Roy Copeland
Tennessee Crime Information Center
Tennessee Bureau of Investigation
Post Office Box 100940
Nashville, TN 37210-0940
(615-741-0437)
FAX (615) 741-4789

TNTBI0000

OPERATIONAL (Quality Control, Validations, Etc.)

Captain Jim Tusan
Memphis Police Department
Room 12-23
201 Poplar Avenue
Memphis, TN 38103
(901-576-2644)

TNMPD0000

Mr. Michael S. Foster
Assistant Director of Data Processing
Metropolitan Police Department
110 Public Square
Nashville, TN 37201
(615-742-7456)

TN0190100

III

(Same as Control Terminal Officer)

TEXAS

CONTROL TERMINAL OFFICER

Mr. David S. Gavin
Chief, Crime Records Division
Texas Department of Public Safety
Post Office Box 4143
Austin, TX 78765-4143
(512-465-2077)
FAX (512) 465-2885

TX0000000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

UTAH

CONTROL TERMINAL OFFICER (Quality Control)

Mr. Richard J. Townsend UTBCI0000
Director
Bureau of Criminal Identification
Utah Department of Public Safety
4501 South 2700 West
Salt Lake City, UT 84119
(801-965-4561)
FAX (801) 965-4749

OPERATIONAL (Validations Only)

Ms. Judy K. Sorenson UTBCI0000
Supervisor
Bureau of Criminal Identification
Utah Department of Public Safety
4501 South 2700 West
Salt Lake City, UT 84119
(801-965-4446)

III

(Same as Control Terminal Officer)

VERMONT

CONTROL TERMINAL OFFICER

Lieutenant Richard D. Boyden VTVSP0000
Director
Vermont Criminal Information Center
Department of Public Safety
Post Office Box 189
Waterbury, VT 05676
(802-244-8727, Ext. 220)
FAX (802) 244-1106

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

VIRGINIA

CONTROL TERMINAL OFFICER

Captain J. S. Conner
Records Management Officer
Department of State Police
Post Office Box 27472
Richmond, VA 23261-7472
(804-674-2021)
FAX (804) 674-2267

VAVSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

WASHINGTON

CONTROL TERMINAL OFFICER

Captain Herbert E. Howe
Commander
Washington State Patrol
Criminal Records Division
QE 02
Olympia, WA 98504
(206-753-6858)
FAX (206) 753-0444

WAWSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

WEST VIRGINIA

CONTROL TERMINAL OFFICER

Corporal R. L. McCallister
Director, Communications Section
West Virginia Division of Public Safety
725 Jefferson Road
South Charleston, WV 25309
(304-746-2154)
FAX (304) 746-2230

WWWSP0000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

2nd Lieutenant D. B. Atkinson
Criminal Identification Bureau
West Virginia Division of Public Safety
725 Jefferson Road
South Charleston, WV 25309
(304-746-2174)

WVWSP0002

WISCONSIN

CONTROL TERMINAL OFFICER

Mr. Robert McGrath
Director
Crime Information Bureau
Division of Law Enforcement Services
Wisconsin Department of Justice
Post Office Box 2718
Madison, WI 53701
(608-266-7399)
No fax available

WI013015Y

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

WYOMING

CONTROL TERMINAL OFFICER

Mr. James M. Wilson
Communications Unit Supervisor
Division of Criminal Investigation
Criminal Justice Information Section
Rogers Building
316 West 22nd Street
Cheyenne, WY 82002-0001
(307-777-7523)
FAX (307) 777-7252

WY0110400

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

III

(Same as above)

PUERTO RICO

Sgt. Sergio Irizarry-Silva
Director
NCIC/NLETS Center
Police of Puerto Rico
G.P.O. Box 70166
San Juan, Puerto Rico 00936
(809-783-7718)
FAX (809) 793-0150

PRPPR0000

U.S. VIRGIN ISLANDS

Mrs. Juliette Francis-Greaux
U.S. Virgin Islands Police Department
Post Office Box 3807
Charlotte Amalie, St. Thomas,
U.S. Virgin Islands 00801
(809-774-6400)
FAX (809) 774-4057

VI0010000

CANADA

S/Sgt. Ross Reed
NCO - I/C CPSIC
Royal Canadian Mounted Police Headquarters
1200 Vanier Parkway
CPS Building, 3rd Floor
Ottawa, Ontario, Canada
K1A 0R2
(613-998-6324)
FAX (613) 993-0218

ON1000000

OPERATIONAL (Quality Control, Validations, Etc.)

(Same as above)

FEDERAL AGENCY CONTACTS

ATF	Mr. Arthur J. Peoples Special Agent in Charge Bureau of Alcohol, Tobacco, and Firearms Systems Support Branch Room 7000 650 Massachusetts Avenue, Northwest Washington, DC 20226 (202-927-8418) FAX (202) 377-7251	DCATF0000
BOM	Dr. William F. Daddio Chief, Security/Internal Review Staff United States Mint Department of the Treasury Room 734-JSB 633 3rd Street, Northwest Washington, DC 20220 (202-376-0592) FAX (202) 376-4976	
BOP	Ms. Harriet Lebowitz NCIC Coordinator U.S. Bureau of Prisons Room 300 320 First Street, Northwest Washington, DC 20534 (202-724-3121) FAX (202) 724-7026	DCDOJ01H5
DC	Mr. Morris M. Pallozzi Director, Office of Enforcement National Marine Fisheries Service National Oceanic and Atmospheric Administration U. S. Department of Commerce, Room 7472 1335 East-West Highway Silver Spring, MD 20910 (301-427-2300) FAX (301) 427-2001	
DEA	SA Patrick H. Doman Special Investigative Support Section Office of Investigative Support Drug Enforcement Administration Washington, DC 20537 (202-307-8841) FAX (202) 307-8931	DCDEA0000

- SMC-HD #8 -

5/13/92

1

224

DI

Mr. Irving D. Tubbs, Jr., Chief
Branch of Law Enforcement
Office of the Secretary
U. S. Department of Interior
Room 5025A
18th and C. Street, N.W.
Washington, DC 20240
(202-208-6319)
FAX (202) 208-6950

DIS

Mr. John F. Donnelly
Director
Defense Investigative Service
1900 Half Street, SW
Washington, DC 20324-1700
(202-475-0966)
FAX (202) 475-2754

DCDIS010R

DOD OIG

Mr. Robert A. Hodge
Assistant Director, Program Analysis Division
Assistant Inspector General for Investigations
U.S. Department of Defense
400 Army Navy Drive, Rm. 901E
Arlington, VA 22202
(202-693-0282)
FAX (202) 614-9501

DOA

Mr. Steve Copeland
Staff Special Agent
General Investigations Division
Office of Inspector General-Investigations, USDA
14th & Independence Avenue, Southwest, Room 425-E
Washington, DC 20250
(202-720-5940)
FAX (202) 720-8697

DCDOAWA00

DOL

Mr. Julian W. De La Rosa
Inspector General
U.S. Department of Labor
Room S-1303
200 Constitution Avenue, Northwest
Washington, DC 20210
(202-523-8760)
FAX (202) 523-9184

DOS

Mrs. Joan A. Lewis
Chief
Management Systems Division
Bureau of Diplomatic Security
U.S. Department of State
6th Floor; SA-10
2121 Virginia Avenue, Northwest
Washington, DC 20520-1001
(202-663-0416)
FAX (202) 663-0466

DCDOS0021

DOT

Mr. H. Rae Scott
Assistant Inspector General
for Investigations, JI-1
Office of Inspector General
U.S. Department of Transportation
400 7th Street, Southwest
Washington, DC 20590
(202-366-1967)
FAX (202) 366-3912

DCDOT02X0

EPA

Mr. Dale Boll (LE-134X)
Director
U. S. EPA/Criminal Investigations Division
401 M Street, S. W.
Washington, DC 20460
(202-260-5262)
FAX (202) 260-6612

COEPA0100

EPA IG

Mr. Daniel S. Sweeney
Assistant Inspector General for Investigations
Environmental Protection Agency (A-109)
401 M Street, Southwest
Washington, DC 20460
(202-382-4109)
FAX (202) 382-6971

FAA

Mr. David A. Smith
Manager, Investigations & Security
Division, ACS 300
Federal Aviation Administration
Department of Transportation
800 Independence Avenue, Southwest
Washington, DC 20591
(202-267-3965)
FAX (202) 267-3961

FDA

Mr. Paul N. Lancaster
Chief, Investigations Unit
Food and Drug Administration
HFA-21 (Park 3-14)
5600 Fishers Lane
Rockville, MD 20857
(301-443-1811)
FAX (301) 443-2505

FPS

Mr. James Jenkins
Director
Support Services Division
Office of Physical Security and Law Enforcement
GSA, PBS, Room 2314
18th and F Streets, Northwest
Washington, DC 20405
(202-501-0265 or FTS 241-0265)
FAX (202) 501-7998 or FTS 241-7998

DCFPS0000

GPO

Mr. Robert A. Blaney
Deputy Director for Security
Security & Support Services, Room A-648
U.S. Government Printing Office
732 North Capitol Street, Northwest
Washington, DC 20401
(202-512-1333 or 1336)
FAX (202) 512-1500

DCGPOWA00

HHS

Mr. Anthony M. Marziani
Director of Computer Techniques Staff
Office of Inspector General
Department of Health and Human Services
Room 5269, North Building
330 Independence Avenue, Southwest
Washington, DC 20201
(202-619-2531 or FTS 269-2531)
FAX (202) 269-0016

DC001057Y

HUD

Mr. Patrick J. Neri
Assistant Inspector General
for Investigations
Office of Inspector General
Department of Housing and Urban Development
Room 8274
451 7th Street, Southwest
Washington, DC 20410
(202-755-6390)
FAX (202) 755-0354

DC001067Y

ICC

Mr. Franklin D. Bail
Chief
Section of Enforcement
Interstate Commerce Commission
12th Street and Constitution Avenue, Northwest
Washington, DC 20423
(202-275-6720)
FAX (202) 275-1201

INS	Mr. Christopher M. Pohl Senior Special Agent Central Office of Investigation U.S. Immigration and Naturalization Service Room 2207 425 I Street, Northwest Washington, DC 20536 (202-514-0747) FAX (202) 514-0764	USINS0000
IRS	Ms. Patti Turner Internal Revenue Service Criminal Investigation Office of Review and Information Systems Management Information Systems Management Branch CI:R:I - Room 2412 1111 Constitution Ave., N.W. Washington, DC 20224 (202-566-3515) or FTS (566-3515) FAX (202) 566-6743	DCIRS9600
NSA	Mr. Samuel Evans Chief, Investigations Division National Security Agency Post Office Box 557 Linthicum Heights, MD 21090 (301-859-6464) No fax available	MDNSA010R
OPM	Mr. Peter Garcia, Assistant Director Office of Federal Investigations USOPM/OFI P.O. Box 886 Washington, DC 20044 (202-376-3800) FAX (202) 376-3840	PAOPM010R
SI	Mr. Ralph M. Smith Chief, Security Services Section Office of Protection Services Smithsonian Institution Suite 7200 955 L'Enfant Plaza Washington, DC 20024 (202-287-3447) FAX (202) 357-4132	DCSI00000

USA	Mr. Jeffery Porter U.S. Army Military Police Operations Agency 4401 Ford Avenue, Suite 225 Alexandria, VA 22302-1432 (703-756-1880) FAX (703) 756-1081	USA000000
USCG	SA Michael D. Murphy U.S. Coast Guard Investigations Washington Field Office Room B-518 2100 Second Street, Southwest Washington, DC 20593-0001 (202-267-2974) FAX (202) 267-4295	DCCG00100
US Courts, Pretrial Services, and Pro- bation Offices	Ms. Jacquelyn C. Kossin Probation Programs Specialist Probation Division Administrative Office of the United States Courts Washington, DC 20544 (202-633-6226) FAX (202) 633-6289	
USM	Mr. George Yurchak Communications Center U.S. Marshals Service Suite 1190E 600 Army Navy Drive Arlington, VA 22202-4210 (202-307-9104) FAX (202) 307-9177	VAUSM0000
USMC	Lt. Tony Bennett Absentee/Deserter Section (MHC) Headquarters, U.S. Marine Corps Attn: Gunnery Sgt. Kenny Wright 3033 Wilson Boulevard Clarendon Square, Room 208 Arlington, VA 22201 (703-640-3976 or 3977) FAX (703) 640-3955	USMC00000
VA	Mr. John H. Baffa Department of Veterans Affairs Deputy Assistant Secretary for Security and Law Enforcement (006S) 810 Vermont Avenue, Northwest Washington, DC 20420 (202-233-4116) FAX (202) 233-4114	DCVA00000

FEDERAL SERVICE COORDINATORS

DOJ	Mr. David M. Taggart, Deputy Director United States Department of Justice Telecommunications Services Staff Information Resources Management Justice Management Division 425 I Street, Northwest, Room 4106 Washington, DC 20530 (202-514-3750) FAX (202) 514-1777	DCDOJ02Y3
NIS and USN	Special Agent Charles A. Palmer Head, Telecommunications Division Naval Investigative Service Headquarters Building 111 Washington, D.C. 20388-2700 (202-433-9300) FAX (202) 433-9322	USNIS0000
OSI and USAF	Ms. Brenda Jones Administrative Operations Controller HQ AFOSI/MCI Building P3 Bolling Air Force Base Washington, DC 20332-6001 (202-767-5199) FAX (202) 767-6554	DCOSI0000
PO	Inspector Rob Chalmers Chief Terminal Officer Postal Inspection Service 475 L'Enfant Plaza West, Southwest Washington, DC 20260-2100 (202-268-4408) FAX (202) 268-4563	DCP000000
USC	Ms. Ellen Mulvenna NCIC Federal Service Coordinator U.S. Customs Data Center Office of Enforcement Systems 7681 Boston Boulevard Springfield, VA 22153 (703-440-6060) FAX (703) 440-6088	VAUSC6001

5/13/92

USSS

SAIC Randall G. Wood
Federal Service Coordinator
U.S. Secret Service
Investigative Support and Research
Division
1800 G Street, Northwest
Room 710
Washington, DC 20223
(202-435-5773)
FAX (202) 343-1201

DCSS17700

5/13/92

2

231

LOCAL AGENCY SERVICE COORDINATORS

Deputy Chief D. A. Whitten
Dallas Police Department
106 S. Harwood, Room 20
Dallas, TX 75201
FAX 214-670-4372

TXDPD0000

Captain Charles J. Brennan
Commanding Officer, PCIC
Philadelphia Police Department
Franklin Square, Room 211
Philadelphia, PA 19106
215-592-5634

PAPEP0000

Mr. Jose M. Camacho
Information Systems Supervisor
Automated Systems Bureau
Metro Dade Police Department
9105 Northwest 25th Street
Miami, FL 33172
305-471-1818

FL0130000

Mr. Leo P. Carroll
Director of Management and
Information Services
New York Division of
Criminal Justice Services
Executive Park Tower
Stuyvesant Plaza
Albany, NY 12203
518-457-2393

NY001015Y



Off-Line Search

Revised October, 1987

The National Crime Information Center (NCIC) is a nationwide on-line computer/telecommunications system which contains millions of stolen property, wanted person, missing person, and unidentified person records that are instantaneously available to local, state, and Federal criminal justice agencies across the United States. On-line inquiries for timely and accurate information can increase the probability of criminal detection. However, during the course of some investigations, information needs may develop which cannot be satisfied by an on-line inquiry. In cases such as these, agencies may request off-line searches of the data base.

An off-line search is a special technique to obtain from the NCIC computer information which cannot be obtained with an on-line inquiry. Off-line searches are used in a variety of circumstances. The results may provide an investigator with information to:

- determine if any agency(s) made an inquiry on a particular individual or item of property.
- place an individual at the scene of a crime or miles away from the scene.
- substantiate or discredit an alibi.
- determine if a record for a person or item of property was previously entered into NCIC and subsequently removed.
- track the route of an individual, e.g., suspects, witnesses, runaways, etc.

NCIC off-line searches use three types of NCIC information:

- The NCIC data base of active records, which is maintained in an on-line mode 24 hours a day, seven days a week.
- The NCIC historical data base, which is maintained off-line on magnetic tape. Historical data includes records

that have been removed from the active data base due to record cancellation, record retention expiration, or record clearance.

- The transaction log which contains historic NCIC transactions.

NCIC off-line search possibilities are infinite. Searches can be limited to a certain time frame, i.e., a particular year(s), day(s), or hour(s), and to the records and/or transactions of a particular state(s), city(s), or agency(s).

An NCIC off-line search can be made with a minimum of one search parameter; however, searches including all available information may be more efficient and effective. Searches can be made on nonunique personal descriptors such as sex, height, weight, estimated age, and hair color to identify a wanted, missing¹, or deceased person; or on a partial license plate number or vehicle identification number (VIN) to identify a vehicle. Gun make, article type, securities descriptors, date of theft, and date of warrant can also be used as off-line search parameters. Inquiries on a large number of securities believed to be stolen can be quickly handled via the off-line search as opposed to time-consuming individual operator on-line inquiries. In some cases, the off-line search may provide identifying data on a suspect(s). Even in cases where all VINs and serial numbers have been obliterated beyond restoration, the off-line search capability has been of value.

NCIC also maintains printed listings of records for persons that are active in the NCIC Wanted Person and Missing Person Files. These printouts are helpful in situations

where a date of birth or other numeric identifier is unavailable for making an on-line inquiry. The lists are printed alphabetically by last name and are updated monthly. Information from the lists are made available to criminal justice agencies by contacting the NCIC Control Room at (202)324-2311.

Let's look at actual cases where the requested off-line search provided vital information that led to the closing of the case. As you will see, each off-line search is unique, thus showing how the scope of a search can be tailored to fit a particular case.

Case #1

One of the more famous investigations NCIC assisted with was the assassination of Martin Luther King, Jr. The investigation centered on a latent fingerprint believed to be from the suspect's left thumb. An off-line search was made of the NCIC Wanted Person File of approximately 25,000 fugitives to retrieve records of all individuals whose left thumb print had a ridge count of 9 through 15. The preliminary search, using only the fingerprint classification code, indicated there were 2,300 such persons listed. The program was then modified to include the other search parameters of age, sex, and race. This reduced the number of possibilities to 1,200 persons.

The information on these 1,200 persons was printed on individual cards and forwarded to the Latent Fingerprint Section of the FBI Identification Division for use in pulling the necessary fingerprint cards against which the latent fingerprint was to be checked. Within the first 100 records examined by the Identification Division, the latent fingerprint was matched with the left thumbprint of James Earl Ray.

Case #2

On July 27, 1986, the family of a 28-year-old woman reported to the Manchester, Tennessee, Police Department that the woman (and her rented automobile) was missing and had not been seen or heard from for four days. Because of suspicious

circumstances surrounding the disappearance, law enforcement officers from local, state, and Federal agencies began a statewide search.

Two days before the missing person report was made, a man was arrested and held in jail in Baltimore, Maryland, on charges of driving under the influence of alcohol and fleeing police. The vehicle he was driving was impounded; an NCIC check produced no record.

On August 1, the FBI office in Tullahoma, Tennessee, assisting in the missing person case, contacted NCIC. A request was made for an off-line search of the NCIC transaction log to determine if any inquiries were made concerning the missing woman or her vehicle during the first four days they were missing. The results of the search produced the inquiry made by the Baltimore police on July 25.

Agents with the Tennessee Bureau of Investigation traveled to Baltimore and arrested the driver of the missing woman's rental car. After subsequent investigations, the authorities learned the location of the woman's body — a wooded area about a mile from the place where she was last seen alive. The body was found tied to a tree with a fatal gunshot to the head.

Case #3

In October, 1984, a double homicide was committed in Bland County, Virginia. The victims had been shot with a .45 caliber automatic pistol; however, the weapon was not recovered at the scene. A joint investigation conducted by local and state authorities developed a suspect who had left the area shortly after the crime was committed. An NCIC off-line search was requested on all inquiries made on either the suspect's name or the vehicle he was operating. The search revealed several inquiries, one of which provided a lead in the case. Follow-up contact with Morgan City and Berwick, Louisiana, police officers revealed that an inquiry on the suspect's vehicle was made after a local vagrant reported that the operator of the vehicle made a

remark about killing someone. Subsequent investigation led to the location of the suspect. Search warrants were obtained and the murder weapon was seized. The man was charged with two counts of capital murder and two counts of using a firearm in the commission of a felony.

Case #4

Investigators with the Auto Theft Unit of the Baltimore City Police Department, Baltimore, Maryland, executed a search warrant at a local body shop as part of an on-going investigation. The search produced a 1977 Corvette. When examining the vehicle, it was learned that the VIN plate did not match the confidential VIN and engine number. There was no active record in NCIC that could be associated with any of the numbers.

On November 8, 1985, NCIC was requested to conduct a search of all purged vehicle records using the confidential VIN. The search produced the record for a vehicle that was entered by the Baltimore County Police Department after it was reported stolen from a new car dealership on June 6, 1977. The record was removed from NCIC in January, 1982, after the standard four-year retention period had expired. As a result of the off-line search, three individuals were arrested immediately and an automobile was recovered with an estimated value of \$10,000.

Case #5

In the next example, NCIC helped solve a case of an unidentified person. On October 17, 1986, the Howard County Sheriff's Office in Fayette, Missouri, entered an unidentified person record for a drowning victim. The body had been floating in the water for five to ten days before its discovery. Considering the bloated condition of the body, the closest

estimates of the man's physical description were entered, as well as the fact that he wore a blue shirt with name "Harvey" imprinted thereon. The cross-search of this record against all missing person records resulted in 13 possible matches; however, none were listed for a man name Harvey and none were identified with the unknown deceased. In this case, an off-line search proved to be the answer. An off-line search was done on all missing person records containing the first name Harvey. That search produced 14 records. Of those, three showed a year of birth that fell within the range indicated in the estimated year of birth of the unidentified person record. After manually comparing the height and scars, only one possible match remained. That missing person record was entered by the Olathe, Kansas, Police Department. The date of last contact with the missing person was four days prior to the estimated date of death of the drowning victim. The Howard County Sheriff's Office subsequently compared dental records and confirmed the match.

The automatic cross-search (mentioned in the beginning of this example) did not match the missing person "Harvey" record because of three factors. First, the physical descriptions of the two were not similar enough to qualify as a possible match. As you may recall, the condition of the body made it difficult to determine actual identifying characteristics. Second, the data in the Miscellaneous Field is not searchable. That data is intended to aid in further identification of an individual. In this case, the name Harvey was included in this Field. Third, obviously there is no Name Field in an unidentified person record. Even though the name did not play a role in the automatic computer match, it proved to be a significant factor in learning the victim's identity through the off-line search.

Conclusion

The NCIC off-line search is a tool designed to assist an investigator by providing lead information. The investigator should furnish to NCIC all available information obtained through the investigation which might lend itself to an off-line search. The NCIC Staff will then assist in determining the feasibility and/or possibility of an off-line search being run. The requests for an off-line search should be directed to the NCIC Training Staff at telephone (202)324-2611 or an administrative message may be sent using DCFBIWAT8 as the destination ORI. The results of the search will be furnished on a computer printout or, if circumstances require, a magnetic tape.

As a means of evaluating the usefulness of the NCIC off-line search program, a survey form is provided with the results of each search. NCIC urges all recipients to complete the form and return it to NCIC as soon as practical. A postage-paid return envelope is included for your convenience.

The continuing need for the off-line search capability along with its proven worth will ensure that it remains a significant investigative aid to all users.

NCIC

Footnote

¹ The availability of all seven personal descriptors (i.e., sex, race, eye and hair color, approximate height and weight, and estimated age) of a person can be used to make an on-line Missing Person File check using the nonunique identifier inquiry capability.

(NCIC) National
Crime
Information
Center

NCIC PUBLICATION REQUEST LIST

NAME: _____
 TITLE: _____
 AGENCY: _____
 ADDRESS: _____
 CITY: _____ STATE: _____ ZIP: _____
 PHONE: (____) _____ ORI: _____

PUBLICATIONS

AMOUNT TITLE

_____ Aircraft Theft(Law Enforcement Bulletin, 10/82)
 _____ Heavy Equipment Theft (LEB 3/81)
 _____ Interstate Identification Index (LEB 1/88)
 _____ Missing Children Act (LEB 1/84)
 _____ Missing...The National Crime Information Center's Missing Person File (LEB 8/82)
 _____ Missing Person Entry Packet (Including Carbon Entry Forms)
 _____ Network Map
 _____ NCIC/More Than Stolen Cars and Wanted Persons (The National Sheriff, June/July 1986)
 _____ On the Cutting Edge-NCIC 2000: Technology Adds a New Weapon to Law Enforcement's Arsenal (The Police Chief, 4/90)
 _____ Trafficking Hot Iron (Construction Equipment, July, 1981)
 _____ Unidentified Person Entry Packet (Including Carbon Entry Forms)
 _____ NCIC/Law Enforcement System is Getting a Major Face-Lift (Technology Magazine, 11/89)
 _____ Report on the Vehicle and Wanted Person Files Survey, April, 1988

AMOUNT TITLE

_____ Areas of Liability (Revised 4/88)
 # _____ Bylaws (October, 1984)
 # _____ Computerized Criminal History Program - Background, Concept, and Policy (March, 1984)
 # _____ Extradition of Wanted Persons and the National Crime Information Center (Revised June, 1983)
 # _____ File Reference Card (Revised February, 1991)
 # _____ Off-Line Search (Revised October 1987)
 # _____ The Investigative Tool, A Guide to Use and Benefits of NCIC (Revised June, 1986)
 # _____ Uniform Offense Codes (Revised October, 1985)
 # _____ Other _____

* - Available for Law Enforcement/Criminal Justice Distribution Only.

NO CHARGE FOR ANY PUBLICATION

NCIC Operating and Code Manuals are available from your Control Terminal Officer. Return this form with your name, address, telephone number and ORI number to: **FOR OFFICIAL USE ONLY**

Federal Bureau of Investigation
 National Crime Information Center
 Room 7233, TL# 245
 Washington, DC 20535
 (202) 324-2711

DRR	BY
DRH	BY
PBO	BY
BKH	BY

236

NCIC ADVISORY POLICY BOARD
SAN ANTONIO, TEXAS
JUNE 3-4, 1992

NCIC STAFF PAPER

TOPIC #11

Consideration of a Comprehensive Security
Policy Document for the NCIC System

BACKGROUND

The NCIC 2000 Risk Analysis, conducted in September, 1988, with the participation of Advisory Policy Board members, Control Terminal Officers (CTOs), and others, prompted the review of security for NCIC 2000 implementation. The goal of the risk analysis was to identify the likelihood of threats to NCIC 2000 assets and cost-effective countermeasures to these threats. The risk analysis effort was based on the NCIC 2000 functionality, the proposed design, and the recommended architecture, and resulted in a draft produced by MITRE Corporation entitled "Risk Analysis of the National Crime Information Center (NCIC) 2000, October, 1989, WP88W00472." This analysis identified intentional disclosure of information by authorized users as the highest risk to the System. The appropriate countermeasures devised to combat unauthorized disclosure was development of improvements in preemployment screening and supervision of terminal operators.

In November, 1989, the Planning and Evaluation (P&E) Ad Hoc Subcommittee began reviewing various documents as background for the development of a comprehensive NCIC 2000 security policy document. Many factors, such as legal security requirements imposed on the NCIC System, existing Board-promulgated security policy, existing FBI security policy which impacts on NCIC operations, and NCIC 2000 concepts and architecture proposals which positively or negatively affect system security were considered during this review. Experience in security and security violation issues by the FBI and NCIC CTOs and previous FBI and state NCIC audit results that pertained to security issues were also included.

During the January, 1990, P&E Subcommittee meeting, members discussed two NCIC Staff Papers entitled "Terminal Operator Background Checks" and "Background for the Consideration of Policy Affecting System Security" and a statistical report titled "Report on the NCIC Terminal Operator Security Survey, June, 1989. The Subcommittee reviewed specific portions of NCIC policy dealing with access controls, dissemination controls, and auditing, with the intent of rewriting existing policy to meet the risks and problems associated with NCIC 2000. As a separate issue, the Subcommittee met with Dr. Peter G. Neumann to discuss

his report entitled "Security Controls for NCIC Computer Use: Federal, State, and Local."

During the March, 1991, P&E Subcommittee meeting, members met with Dr. Neumann to discuss security issues pertaining to NCIC 2000. The MITRE Corporation made a presentation concerning security for NCIC 2000 from the perspective of the NCIC 2000 study. Their presentation was endorsed without any changes by the Subcommittee. The Subcommittee also considered this comprehensive security document in conjunction with the above presentations.

The Advisory Policy Board reviewed this document at its December 4-5, 1991, meeting. Based upon the P&E Subcommittee's comments the Board made changes to the document. All policy statements are italicized and changes since last Board meeting appears in shaded text while text being removed is highlighted with a line through it. The P&E Subcommittee reviewed this document at its April, 1992, meeting. Recommendations appear in text blocks.

DISCUSSION

This section addresses specific security issues which were considered by the P&E Subcommittee. Each topic contains a rewrite of a specific area of security. If considered necessary, a discussion is included of related issues that may be considered in addition to those matters already addressed.

I. Personnel Security

NCIC policy regarding personnel security currently is directed only to those agencies having terminals with access to the Interstate Identification Index (III) information and provides nonspecific guidance.

After discussing the previously mentioned staff papers, the P&E Subcommittee agreed that specific personnel security measures must be met for any criminal justice or noncriminal justice employee who will access not only the III data base but also the NCIC data bases. The Subcommittee adopted specific language as follows:

Background Screening

Thorough background screening by the employing agency of personnel is required. State and national III record checks by fingerprint identification must be conducted for terminal operators, programmers, and other persons employed or utilized to effectuate access to or initiate transmission of NCIC information. Good management practices dictate record checks should be completed prior to employment.

Appropriate background investigations must be conducted on all NCIC terminal operators, including submission of a completed applicant fingerprint card to the FBI Identification

Division through the state identification bureau. When a request for operator access to NCIC is received by the CTA, before system access is granted:

1. The CTA and/or the employing agency staff must check state and national arrest and fugitive files.
2. If a record of any kind is found, access will not be granted. The agency to which the applicant has applied for employment and/or NCIC access will be formally notified indicating NCIC access will be delayed pending review of arrest and fugitive records.
3. When identification of the applicant has been established by fingerprint comparison and he/she appears to be a fugitive or to have an arrest history for a felony or serious misdemeanor, an agency head or their designee will review the matter. If the applicant is found to be a fugitive from justice, or to have been convicted of a felony or serious misdemeanor, the matter will be referred to the executive head of the CTA or his/her designee.
4. If a determination is made that NCIC access by the applicant would not be in the public interest, such access will be denied and the applicant's appointing authority will be notified in writing of the access denial.

The Board adopted the following changes due to the fact that "termination" is a form of disciplinary action:

Discipline or Termination of Policy Violators

Each criminal justice agency authorized to receive NCIC information must have appropriate written standards for discipline and/or termination of NCIC policy violators.

The Board also recommended in June, 1990, that legislation should be directed at the broader category of NCIC information and misuse of the System to include improper alteration of records instead of unauthorized dissemination of III information only. A Staff Paper titled "Federal Legislation to Criminalize Misuse of NCIC" was presented at the fall, 1990, round of RWG meetings for review and comments. A revised copy of this Staff Paper was included in the P&E agenda as Topic #7, for the December, 1990, P&E Subcommittee meeting. The P&E Subcommittee endorsed this legislation as proposed. During the December, 1990, Advisory Policy Board meeting, the Board accepted the P&E Subcommittee's recommendation for this proposal.

II. Physical Security

The NCIC User Agreement states that "an agency participating in the NCIC as a CTA and other agencies with direct telecommunications line access must assume

responsibility for and enforce system security with regard to all other agencies which it, in turn, services." The User Agreement further elaborates on this requirement to "include all places where terminal devices are located" for agencies that receive III information.

The P&E Subcommittee recommended that specific language be added to the above requirement to specifically identify NCIC system security. The modification is as follows:

The NCIC User Agreement would require that "an agency participating in the NCIC as a CTA and other agencies with direct telecommunications line access must assume responsibility for and enforce NCIC System security with regard to all other agencies which it, in turn, services."

The P&E Subcommittee recommended that physical security requirement be extended to state that specific security standards must be met in instances where agencies access NCIC and/or III information. These standards include:

A. Computer Site

The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

B. Visitors

All visitors to computer centers and/or terminal areas must be accompanied by staff personnel at all times.

C. Authorized Employees

Agencies having terminals with access to NCIC and III information must have terminal operators screened according to specified guidelines. Access to the terminal area should also be restricted to the minimum number of authorized employees needed to complete the work.

In addition to the above-mentioned physical security policy, the following are also relevant to physical security.

1. CTAs should have procedures in place to monitor all security policies; e.g., through Terminal Agency Coordinators, state audit programs, etc.
2. Operators should use the terminal only for those purposes for which they are authorized.
3. CTAs should have procedures in place regarding changing of passwords, logons, etc., in relation to terminated employees.

III. User Authorization

A. Originating Agency Identifier

System access is controlled through assignment and use of Originating Agency Identifiers (ORI). ORIs are assigned by the FBI NCIC based on the FBI NCIC ORI Policy approved by the NCIC Advisory Policy Board on June 17, 1981, and subsequently modified as new requirements dictated. This policy established qualifying criteria for access and provided for several levels of access, including access to particular files; e.g., certain nongovernmental police departments having inquiry only access to "hot" files.

The P&E Subcommittee adopted the following guidelines for use of the ORI: The ORI must be used in each transaction on the System, and thereby serve to ensure the proper level of access in each transaction. At the initial submission of a transaction into the System, the ORI is automatically referenced to the relevant state telecommunications circuit. The CTA must further ensure that the ORI is in fact originating from the assigned location(s) within the state. This will prevent one agency from masquerading as another. Additionally, this will ensure that an agency wishing to modify or cancel an NCIC entry is the entering agency.

B. User Agreements

The NCIC system has operated under a shared management concept between the FBI and state users. The NCIC Advisory Policy Board established a goal of having a single state agency in each state assume responsibility as the NCIC CTA for the state, through and by which NCIC users in that state would access NCIC. The Board approved the CTA concept in order to unify responsibility for system user discipline and adherence to System procedures and policies within each state.

The responsibilities of the CTA are detailed in several documents (NCIC Operating Manual; Minutes of the NCIC Advisory Policy Board; Bylaws for the NCIC Advisory Policy Board and RWGs; Title 28, Code of Federal Regulations, Part 20; NCIC Standards as recommended by the NCIC Advisory Policy Board and approved by the FBI Director; and applicable Federal and state laws) related to the NCIC System.

Current NCIC policy requires each CTA to sign a written agreement of which the above-mentioned documents are incorporated before participation in the III program. This policy was further extended to require similar agreements between CTAs and terminal agencies as well as terminal and nonterminal agencies if the agencies are capable of accessing III data. The P&E Subcommittee modified the above policy as follows:

Each CTA must sign a written agreement, of which these documents are incorporated, with the NCIC to conform with system policy before participating in the NCIC and III programs. This allows for control over the data and gives assurance of system security.

To further control the data and System security, each CTA must prepare and execute a written agreement containing similar provisions to the agreement by the states and NCIC, with each criminal justice agency having a terminal device capable of accessing NCIC and III data within that state.

Each terminal agency must also prepare and execute, ~~in the absence of such an agreement with the CTA~~, a written agreement, approved by the CTA, for each nonterminal agency for whom they provide NCIC and III service which contains similar provisions to the agreement between the terminal agency and CTA.

During its December, 1991, meeting, the Board approved a motion that tasked the P&E Subcommittee with drafting a model user agreement that is designed to be completed between the CTA and agencies that only receive hot file information and are not under the management control of a criminal justice agency.

At the April, 1992, P&E Subcommittee meeting, members approved the following motion that would apply to agreements between the CTA and terminal agency/nonterminal agency, terminal agency and nonterminal agency, and CTA and agencies that only receive hot file information and are not under the management control of a criminal justice agency:

"Any agency that requests access to NCIC databases must enter into a written agreement with the Control Terminal Agency or Federal Service Coordinator or the terminal agency that will provide said access. This written agreement will delineate the NCIC databases to which the agency will have access and the NCIC policies to which the agency must adhere to ensure continuation of said file access. These policies include:

- Timeliness - availability (including priority)
- Quality assurance
- Validation
- Ten minute hit confirmation
- Security
- Dissemination
- Audit
- Training
- Screening (pre-employment, pre-access)
- Logging
- Use of system

This agreement will also delineate the process by which local user agencies may appeal NCIC service related decisions made by the agency that provides them direct terminal access as provided by this agreement."

The Subcommittee also recommended that the NCIC Staff draft minimal language for this type of agreement (including necessary attachments) for CTAs and FSCs to utilize if they do not already have this type of agreement. This draft will be presented to the Planning & Evaluation Subcommittee for approval prior to its presentation to the Advisory Policy Board at its

December, 1992, meeting. The Subcommittee specified that the new agreement should be less voluminous and more to the point than the current User Agreement executed by the NCIC and the Control Terminal Agencies.

C. Management Control

Current NCIC policy requires management control with reference only to III record information. The P&E Subcommittee extended this requirement to NCIC and III information as follows:

Management control is defined as the authority to set and enforce (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operation of computers, circuits and telecommunications terminals used to process, store, or transmit ~~"hot" file and III~~ record information and guarantees the priority service needed by the criminal justice community.

Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the ~~"hot" file and III~~ programs. A criminal justice agency must have a written agreement with the noncriminal justice agency operating the data center which assures that the criminal justice agency has management control as defined above.

All computers, electronic switches, and terminal devices interfaced directly with the NCIC computer for the access of ~~NCIC "hot" file and III~~ information must be under the management control of criminal justice agencies. Similarly, satellite computers, electronic switches, and terminal devices accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency. This management requirement applies to all interfaced agencies. The following are approved ~~to access~~ to access ~~to NCIC~~ ~~and III~~ but do not meet the definition of a criminal justice agency. Management control extends to these specific exceptions:

Department of Defense (DOD), Central Intelligence Agency (CIA), and Office of Personnel Management (OPM) - Public Law 99-169, "Security Clearance Information Act (SCIA)," authorizes these noncriminal justice agencies to review all NCIC files, including III, for investigations on individuals who will have access to classified information or be assigned to or retained in sensitive national security duties.

National Center for Missing and Exploited Children (NCMEC) - An opinion by the Department of Justice, Office of the Deputy Assistant Attorney General, Office of Legal Counsel, authorizes this noncriminal justice agency access to the NCIC Missing Person and Unidentified Persons Files in order to provide information, counseling, and technical services at the national level on missing and exploited children.

- * National Insurance Crime Bureau (NICB) - When the NCIC was established in 1967, NICB, a noncriminal justice agency supported by insurance companies, made available all of its stolen vehicle records to help establish a data base in the NCIC Vehicle File. As a result of this cooperative effort, NICB was permitted access to*

the Vehicle File as an exception to the NCIC policy requiring this information be restricted to criminal justice agencies. NICB is permitted to make vehicle inquiries, locate vehicles, and modify the NICB interest field.

- * On January 1, 1992, NATB merged with the Insurance Crime Prevention Institute to form the National Insurance Crime Bureau (NICB). The details of this change are covered in a separate Staff Paper for this meeting.

Department of Motor Vehicles (DMV) - The NCIC Advisory Policy Board approved access for this noncriminal justice agency to the NCIC "hot" files in order to accommodate the volume of inquiries that would otherwise have to be handled by another criminal justice agency.

All of these agencies have special designated ORI assignments which permit access only to the files for which they have been authorized. (All criminal justice agencies and the above-mentioned excepted noncriminal justice agencies will be referred to as authorized users.)

IV. Technical Security

A. Dial-Up Access

Dial-up access is the process of accessing NCIC and III files using nondedicated telephone communications. Denial of dial-up access to the NCIC System was based on several reasons.

1. Security - Without ample precautions, a dial-up feature provides a window into a computer system.
2. Cost - An agency with NCIC access requirements great enough to warrant a circuit to NCIC would need so much circuit connect time that the aggregate of the per minute dial-up charges would far exceed the cost of a dedicated circuit.
3. Reliability - Dial-up circuits do not have as high a conditioning level as a dedicated circuit.
4. Diagnostics - The error detection software and hardware in use on the dedicated circuits would not be as effective on a dial-up circuit.

The Board retained the dial-up prohibition and clarified two exceptions as follows:

"The policy was restated to prohibit any access by dial-up means which would operate on a continuing basis and would allow access to the NCIC System either

directly or through a state system. This would not prohibit dial-up access for temporary emergency communications or for diagnostic purposes provided that appropriate security measures are in place."

A major consideration in the Board's deliberation was that the external political perception of the NCIC System might be equated to that of private credit bureaus and other "breakins" occurring during that period. Several states argued that they had been required to deal with the issues and had been successful in maintaining dedicated circuits and other states should do the same.

At the fall, 1990, round of meetings, the RWGs considered two proposals for expanded dial-up access. One proposal dealt with access for training purposes only while the other presented generalized dial-up access as a cost savings measure. The RWGs withheld action on these proposals pending a review by the P&E Subcommittee to assess technological controls available to protect dial-up circuits and the policy guidelines as to when it can be used.

At the March, 1991, P&E Subcommittee meeting, the dial-up issue was readdressed. Various technological controls were considered as well as the financial advantages versus the possible adverse political repercussions. The Subcommittee passed a motion as follows:

"That further consideration not be given in view of the many concerns discussed by the Subcommittee and minimal stated interest and that the subject not be addressed again without additional evidence presenting substantial support for dial-up access."

While such additional evidence has not been presented other than monetary savings, two other written requests and one oral request have been received requesting generalized dial-up access. The basic premise of these requests is that sufficient technical and procedural controls exist to effectively secure dial-up access.

The P&E Subcommittee again considered the dial-up issue in light of these new requests at the May, 1991, meeting. This resulted in a recommendation to the Board that there be no change to the existing policy concerning dial-up access. The Board considered this recommendation at its June, 1991, meeting and referred it to the RWGs for input on how to protect dial-up access. At the fall, 1991 round of RWG meetings the recommendations were: Northeastern and Western voted to retain the current policy limiting dial-up to temporary emergency and diagnostic purposes, Southern extended current policy to include CTA conducted training, and North Central endorsed general dial-up access with adequate security to include all or some of specified security conventions; i.e., identification/authentica-

tion (user ID and password), encryption, automated or manual callback, or caller ID.

At its November, 1991, meeting, the P&E Subcommittee passed a motion not to modify the current dial-up policy because there was not any new or additional information regarding the technical security required to protect the dial-up circuits.

During the December, 1991, Advisory Policy Board meeting, the Board approved a motion requesting that Regional Chairmen survey all of the state and local representatives and bring to the Chairmen of the P&E Subcommittee any information about new technology which provides for secure dial-up.

At its April, 1992, meeting, the P&E Subcommittee agreed to recommend that the Board authorize the P&E Subcommittee to develop a minimum level of security for dial-up access (with human intervention being a minimum) and that beyond that, the CTA must document and approve each use of dial-up. The documentation must be maintained by the CTA and will include the authorization of the user, the user agency, the purpose of use, the frequency of use, and the location of the dial-up site.

B. Logging

FBI NCIC maintains an automated log of all "hot" file transactions for ten years. III transactions are maintained in two forms: 1) A transaction log which is maintained for ten years and 2) A dissemination log which is maintained indefinitely. NCIC logging requirements for CTAs presently pertain only to the III files. The logs must notate the individual making the request for the record and must be maintained for a minimum of one year. The P&E Subcommittee revised this requirement as follows:

The CTA shall ensure that all NCIC "hot" file transactions and III transactions (both QH and QR) originating from terminal devices which access the NCIC through the state system be maintained on an automated log. The "hot" file portion of this log must be maintained for a minimum of six months and the III portion must be maintained for a minimum of one year. This automated log must in some way identify the operator on III transactions as well as the agency authorizing all transactions. III logs must in some way identify the requester and secondary recipient. This information can be captured at logon and can be a name, badge number, serial number, or other unique number.

One other consideration might be addressed when defining what the automated log must include. In addition to capturing the operator and authorizing agency on the automated

log, capturing the entire transaction, physical line or address identity, and date and time stamp would further enhance the audit trail of a particular transaction.

V. Dissemination

A. General Dissemination

The NCIC Operating Manual states that *"The data stored in the NCIC is documented criminal justice information and this information must be protected to ensure correct, legal, and efficient dissemination and use...The individual receiving a request for criminal justice information must ensure that the person requesting the information is authorized to receive the data. The stored data in NCIC is sensitive and should be treated accordingly, and unauthorized request or receipt of NCIC material could result in criminal proceedings...If no state/local law or policy prohibition exists, indirect dissemination of NCIC records, other than III, is discretionary with the state control terminal agency."*

B. III Dissemination

The NCIC Computerized Criminal History Program Background, Concept and Policy Paper states that *copies of III data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of the data.*

The P&E Subcommittee recommended no changes to the above NCIC policy. However, one issue that may be relevant to the III dissemination portion is the appropriate destruction of III data.

C. III Record Retention

The P&E Subcommittee recommended that *III records be maintained in a secure records environment. Such storage of records will be retained for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal record files where they are retained.*

D. III Record Disposition/Destruction

The P&E Subcommittee recommended that *when retention of III records is no longer required, final disposition will be accomplished in a secure manner so as to preclude unauthorized access/use.*

VI. Audit

Current NCIC policy requires all CTAs and SCs to institute a program of systematic self-audits. In addition to audits conducted by all CTAs and SCs, each CTA/SC shall be audited at least once every two years by the NCIC Staff. The objective of this audit is to verify adherence to NCIC policy and regulations and is termed a compliance audit.

All CTAs and other criminal justice agencies having direct access to III data from the System shall permit an inspection team appointed by the NCIC Advisory Policy Board to conduct appropriate inquiries with regard to any allegations of security violations. The inspection team shall include at least one representative of the FBI NCIC. All results of the investigation conducted shall be reported to the Advisory Policy Board with appropriate recommendations.

The P&E Subcommittee revised the above policy, with emphasis on the clarification of NCIC and state audit requirements, as follows:

Each Control Terminal Agency (CTA) and Service Coordinator (SC) is required to establish a system to biennially audit every terminal agency to ensure compliance with state and NCIC policy and regulations. In addition to the audits conducted by all CTAs and SCs, each CTA/SC shall be audited at least once every two years by the NCIC Staff. The objective of this audit is to verify adherence to NCIC policy and regulations and is termed a compliance audit. This audit shall include a sample of state and local criminal justice agencies. A compliance audit may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance.

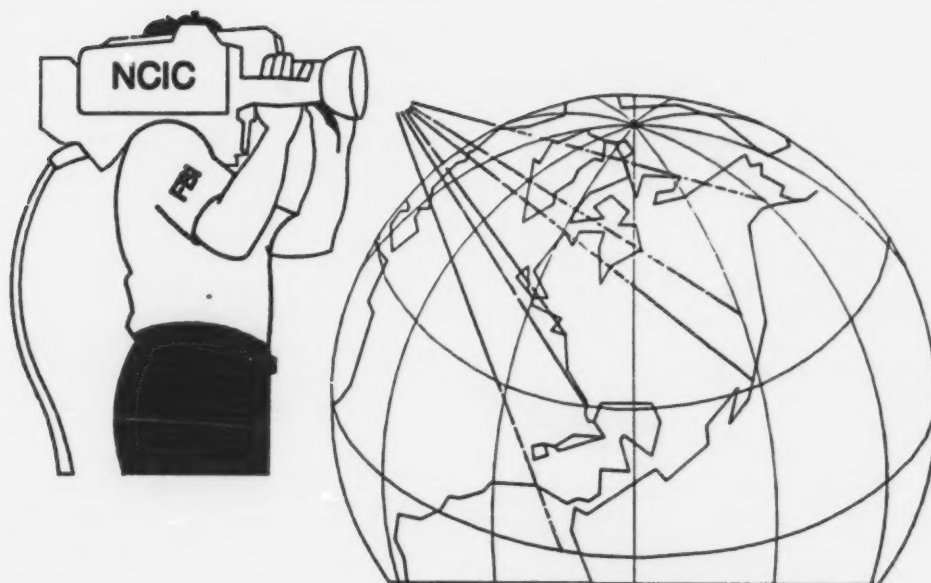
All CTAs and other criminal justice agencies having direct access to NCIC and III data from the System shall permit an inspection team appointed by the NCIC Advisory Policy Board to conduct appropriate inquiries with regard to any allegations of security violations. The inspection team shall include at least one representative of the FBI NCIC. All results of the investigation conducted shall be reported to the Advisory Policy Board with appropriate recommendations.

The Advisory Policy Board approved the following sections of this document at its December, 1991, meeting:

Section I, Personal Security
Section II, Physical Security
Section III, User Authorization, Parts A & B
Section V, Dissemination
Section VI, Audit

Section III, User Authorization, Part C, Management Control, and all of Section IV, Technical Security, was not approved by the Board pending the outcome of the management control and dial-up issues. The P&E Subcommittee's recommendations on management control are included in Section III, User Authorization, Part B, and their recommendations on dial-up are included in Section IV, Technical Security, Part A of this paper. The Board is requested to review the P&E Subcommittee's changes to the document which were made in response to the Board's recommendations.

NATIONAL CRIME INFORMATION CENTER TRAINING VIDEOS



NCIC VIDEOS PRODUCED AS OF MARCH 1992

1. **THE INVESTIGATIVE OFFLINE SEARCH**
***FBI/NCIC**
2. **NCIC HIT CONFIRMATION FOR PATROL OFFICERS**
3. **NCIC VALIDATION POLICY**
***NCIC AND NEW YORK STATE POLICE**
4. **NCIC OVERVIEW**
5. **NCIC WANTED PERSON FILE**
6. **NCIC PACKING THE RECORD**
***NCIC AND ARIZONA DEPT. OF PUBLIC SAFETY**
7. **NCIC UNIDENTIFIED PERSON FILE**
8. **NCIC RESPONSIBILITIES FOR THE AGENCY ADMINISTRATOR**
9. **NCIC VEHICLE FILE FOR PATROL OFFICERS**
***NCIC AND LOS ANGELES POLICE DEPARTMENT**
10. **NCIC AND MISSING CHILDREN**
***NCIC AND MARYLAND STATE POLICE**
11. **NCIC 2000**
12. **NCIC VEHICLE FILE- "THE WINNING TEAM"**
***NCIC AND INDIANA STATE POLICE**
13. **NCIC BOAT FILE**
***NCIC AND FLORIDA DEPT. OF LAW ENFORCEMENT**
14. **NCIC SYSTEM SECURITY**
***NCIC AND MARYLAND STATE POLICE**
15. **INTERSTATE IDENTIFICATION INDEX**
***NCIC AND NORTH CAROLINA JUSTICE ACADEMY**
16. **NCIC GUN FILE**
***NCIC AND HONOLULU POLICE DEPARTMENT**
17. **NCIC/ATF VIOLENT FELON FILE**
***NCIC AND CHICAGO POLICE DEPARTMENT**

**NCIC IS LOOKING FOR LAW ENFORCEMENT AGENCIES INTERESTED IN
COPRODUCING NCIC TRAINING VIDEOS. FOR MORE INFORMATION REGARDING
THIS OR ANY OF THE AVAILABLE VIDEOS, PLEASE CONTACT:
MARIE E. BERNOI, NCIC VIDEO TRAINING COORDINATOR AT
(202)324-2011.**

**NATIONAL CRIME INFORMATION CENTER OFFERS TRAINING VIDEOS
FOR THE CRIMINAL JUSTICE COMMUNITY**

The FBI's National Crime Information Center (NCIC) has produced 17 training videos to be viewed by NCIC users throughout the criminal justice system. These videos present critical information concerning missing children, wanted persons, unidentified persons, and stolen property. Major policy issues, such as hit confirmation and data quality, are also addressed.

The NCIC training videos are widely used by law enforcement agencies and have been successfully included in training programs for prosecutors, corrections officers, and employees of local, state, and Federal court systems.

The videos have made positive contributions to criminal justice training across the country. For example, William Masters of the California Commission on Peace Officer Standards and Training says, "NCIC training videos are a very informative and effective training tool."

Many of the videos are also being aired on the Law Enforcement Television Network (LETN). This national recognition has provided an awareness of training opportunities and has created an increased interest in NCIC throughout the criminal justice system.

"NCIC provides an invaluable service to the law enforcement community through their creative and informative training videos," states Dave Smith of LETN.

Wide distribution of these videos will continue to enhance the effective use of NCIC. The training videos range from 5 to 15 minutes in length and can be used in a variety of training situations. For example, roll call training in police departments requires clear and concise information that can be provided in a relatively short amount of time. NCIC training videos are ideal for situations in which time and quality are essential.

Copies of the NCIC training videos may be purchased through the National Audiovisual Center. They will be grouped on single VHS tapes in the following sets:

<u>ORDER #</u>	<u>TITLES</u>	<u>PRICE</u>
A18852	NCIC Overview	\$15.00/\$30.00 *
A18853	NCIC Vehicle File NCIC Vehicle File "The Winning Team" NCIC Boat File	\$35.00
A18854	NCIC Hit Confirmation NCIC Validation Policy NCIC Responsibilities for the Agency Administrator	\$35.00
A18855	NCIC Missing Children NCIC Unidentified Person File NCIC Wanted Person File	\$35.00
A18856	NCIC Packing the Record NCIC Investigative Off-Line Search	\$35.00
A18858	NLETS The Vital Link - overview	\$15.00/\$30.00 *
A18971	NCIC SYSTEM SECURITY INTERSTATE IDENTIFICATION INDEX	\$35.00
A19068	NCIC/ATF VIOLENT FELON FILE NCIC GUN FILE	\$35.00

*IF YOU ORDER ONE OR MORE \$35.00 PROGRAMS YOU MAY PURCHASE ONE OR BOTH OVERVIEW PROGRAMS AT \$15.00 EACH. IF YOU PURCHASE ONLY OVERVIEW PROGRAMS THE COST IS \$30.00 EACH.

*NOTE: CREDIT CARD ORDERS MAY BE MADE ON MASTERCARD AND VISA BY CALLING 1-800-788-6282. CHECKS, MONEY ORDERS, OR PURCHASE ORDERS MAY BE SENT TO THE FOLLOWING ADDRESS:

National Audiovisual Center
Customer Service Section
8700 Edgeworth Drive
Capitol Heights, MD. 20743-3701

FOR FURTHER INFORMATION, CALL (301)763-1896.

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: HIT CONFIRMATION

TITLE OF INSTRUCTION:

HIT CONFIRMATION

TIME ALLOTTED:

30 MINUTES

TARGET GROUP:

FULL ACCESS TERMINAL
OPERATORS

INSTRUCTOR:

METHOD OF INSTRUCTION:

LECTURE, OVERHEAD
TRANSPARENCIES, AND VIDEO
TRAINING TAPE

DATE:

7/1/92

NCIC HIT CONFIRMATION LESSON PLAN TABLE OF CONTENTS

STATEMENT OF GOAL AND OBJECTIVES	HC-1
CRITERION TEST	HC-2
CRITERION TEST ANSWERS	HC-3
ITEMS AND MATERIALS	HC-5
INTRODUCTION	HC-6
DEFINITION OF A HIT	HC-6
NCIC TEN-MINUTE HIT CONFIRMATION POLICY	HC-6
THE HIT CONFIRMATION PROCESS	HC-7
Inquiring Agency	HC-7
Entering Agency	HC-8
DOCUMENTATION OF THE HIT CONFIRMATION PROCESS	HC-9
24-HOUR HIT CONFIRMATION CAPABILITY	HC-10
24-hour agencies with one terminal	HC-10
24-hour agencies with multiple terminals	HC-10
Non-24-hour terminal agencies	HC-10
24-hour nonterminal agencies	HC-11
Non-24-hour nonterminal agencies	HC-11
PROBABLE CAUSE	HC-12
CONCLUSION	HC-13
BIBLIOGRAPHY	HC-14

STATEMENT OF GOAL AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator critical information on hit confirmation policies and procedures.

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the operator will be able to:

1. Define an NCIC hit.
2. Describe the Ten-Minute Hit Confirmation policy.
3. Name the steps in confirming a hit for: (a) the inquiring agency and (b) the entering agency.
4. Describe the 24-hour availability policy for hit confirmations.
5. Be aware that an NCIC hit is not probable cause for arresting or seizing property.

CRITERION TEST

1. Define an NCIC hit.
2. Name the steps involved in confirming a hit for:
(a) the inquiring agency and (b) the entering agency.
3. Explain why documentation of confirmed hits is essential.
4. Describe the Ten-Minute Hit Confirmation policy.
5. List the methods in which 24-hour nonterminal agencies can ensure 24-hour hit confirmation coverage.
6. An NCIC hit alone is probable cause to arrest.
 - A. True
 - B. False

CRITERION TEST ANSWERS

1. A hit is a positive response from NCIC in which the person or property inquired upon appears to match the person or property contained in the response.
2. a. The inquiring agency must:
 1. Contact the agency that entered the record to confirm the information.
 2. Ensure that the person or property inquired about is identical to the person or property identified in the record.
 3. Ensure that the warrant, missing person report, or theft report is still outstanding.
 4. Obtain: (1) a decision regarding the extradition of a wanted person, or (2) information regarding the return of the missing person to the appropriate authorities, or (3) information regarding the return of stolen property to its rightful owner.
- b. The entering agency, in response to a hit confirmation request from the inquiring agency, must:
 1. Provide, within 10 minutes, either a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject the action.
 2. Review all available information, including case files, warrants, and all other information that is relevant to identifying the person or property to ensure that a proper response is given.
3. Documentation of confirmed hits is essential in that it may be critical to the success of defending a later claim of misidentification.
4. An originating agency must, within ten minutes, furnish to an agency requesting a record confirmation; a response indicating a positive or negative confirmation or a notice of the specific amount of time necessary to confirm or reject.

An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to their Control Terminal Agency (CTA) or Service Coordinator (SC) and to the CTA or SC responsible for the agency holding the record.

If a CTA fails to ensure compliance with this policy, the agency requesting confirmation will notify FBI NCIC by a third message with a copy to the CTA involved. Such notice will result in imposition of sanctions as approved by the NCIC Advisory Policy Board.

5. Hit confirmation coverage may be provided for 24-hour non-terminal agencies by:
 1. Programmatic routing of all hit confirmation requests to a designated terminal agency.
 2. Placing in the Miscellaneous Field of the NCIC record the telephone number of the nonterminal agency.
6. False. An NCIC hit is not probable cause for arresting or seizing property.

ITEMS AND MATERIALS

Overhead projector and screen

Overhead Transparencies:

- HC-OH #1 - Title of Program
- HC-OH #2 - Montage of False Arrests
- HC-OH #3 - Confirming a Hit
- HC-OH #4 - NLETS YQ Format
- HC-OH #5 - NLETS YR Format
- HC-OH #6 - Course Summary

Handout Materials:

- HC-HD #1 - "Mistaken Identity Results in 18-Day Stay in D.C. Jail."
- HC-HD #2 - "Areas of Liability"
- HC-HD #3 - "Roberto Hernandez Battles His Arresting Similarities to a Wanted Man with the Same Name."
- HC-HD #4 - "A Hit and an Error."
- HC-HD #5 - "Loss of FBI Computer Leaves a Void in Bamberg County Law Enforcement."
- HC-HD #6 - U.S. v. Hensley, 83 L.Ed.2d. 604 (1985).

VCR and Monitor

Videotape:

NCIC Hit Confirmation

I. INTRODUCTION

REFERENCES

THIS 30-MINUTE BLOCK OF INSTRUCTION HAS BEEN DESIGNED TO PROVIDE THE TERMINAL OPERATOR CRITICAL INFORMATION ON HIT CONFIRMATION POLICIES AND PROCEDURES.

OH #1

Over one million inquiries are made daily into the National Crime Information Center (NCIC). Some of these inquiries yield positive responses or "hits" from the NCIC System. In order to ensure that criminal justice agencies respond appropriately to these hits, the Advisory Policy Board (APB) has established specific policies and procedures. Adherence to the established policies will help criminal justice agencies avoid costly lawsuits and penalties.

OH #2
HD #1,2
3,4

II. DEFINITION OF A HIT

IO #1

A hit is a positive response from NCIC in which the person or property inquired about appears to match the person or property contained in the response.

III. NCIC TEN-MINUTE HIT CONFIRMATION POLICY

IO #2

NCIC has established a specific policy known as the NCIC Ten-Minute Hit Confirmation Policy. This policy is designed to ensure that appropriate

action is taken whenever a hit is received from NCIC.

The NCIC Operating Manual contains the NCIC Ten-Minute Hit Confirmation Policy. The policy reads as follows:

1. An originating agency must within ten minutes furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a notice of the specific amount of time necessary to confirm or reject.
2. An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to its Control Terminal Agency (CTA) or Service Coordinator (SC) and to the CTA or SC responsible for the agency holding the record
3. If a CTA fails to ensure compliance with this policy, the agency requesting confirmation will notify FBI NCIC by a third message with a copy to the CTA involved. Such notice will result in imposition of sanctions as approved by the NCIC Advisory Policy Board.

IV. THE HIT CONFIRMATION PROCESS

IO #3

The hit confirmation process begins when the inquiring agency receiving the hit contacts the agency that entered the record. The inquiring agency must:

OH #3

1. Contact the agency that entered the record to confirm the information.
2. Ensure that the person or property inquired about is identical to the person or property identified in the record.
3. Ensure that the warrant, missing person report, or theft report is still outstanding.

4. Obtain: (1) a decision regarding the extradition of a wanted person, or (2) information regarding the return of the missing person to the appropriate authorities, or (3) information regarding the return of stolen property to its rightful owner.

INSTRUCTOR'S NOTE: AN AGENCY NEED NOT CONFIRM A WANTED PERSON RECORD WHEN THE AGENCY IS OUTSIDE OF ANY EXTRADITION LIMITATIONS INDICATED IN THE MISCELLANEOUS FIELD OF THE RECORD. HOWEVER, IF THE CODE "NOAH" (NOTIFY ORI OF ALL HITS) IS IN THE MISCELLANEOUS FIELD, CONTACT THE ORI OF THE RECORD AND FURNISH DETAILS CONCERNING THE INQUIRY.

The entering agency, in response to a hit confirmation request from the inquiring agency, must:

1. Provide, within 10 minutes, either a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject the action.
2. Review all available information, including case files, warrants, and all other information that is relevant to identifying the person or property to ensure that a proper response is given.

Entering agencies should be aware that hit confirmation is especially critical with regard to the Wanted Person File. In instances where the extradition information is not readily available, the entering agency should indicate the specific amount of time needed to obtain extradition information.

V. DOCUMENTATION OF THE HIT CONFIRMATION PROCESS

All hit confirmation teletypes should be retained, and precise notes should be made on the printout concerning how, when, and to whom the information is given. The printout should be dated, initialed, and kept in the case file.

The "YQ" format, available through the National Law Enforcement Telecommunications System (NLETS), may be used by the inquiring agency to send hit confirmation requests. The "YR" format, also available through NLETS, may be used by the entering agency to respond to hit confirmation requests.

OH #4

OH #5

Hit confirmation requests and verification may also be made by telephone. Both the inquiring and entering agencies should obtain documentation in the event the telephone is used. Sources of documentation include:

1. YQ, YR or other teletypes sent as final confirmation,
2. fax messages sent as final confirmation,
3. dispatcher audio tape recordings.

Documentation of the confirmed hit is essential in that it may be critical to the success of defending a later claim of misidentification.

VI. 24-HOUR HIT CONFIRMATION CAPABILITY

IO #4

To ensure that hit confirmation is available promptly, agencies that enter records in NCIC must be able to provide a hit confirmation response within 10 minutes, 24 hours a day, every day of the year.

Hit confirmation coverage may be provided for 24-hour agencies with one terminal by:

1. Programmatic routing of all hit confirmation requests to the terminal.

Hit confirmation coverage may be provided for 24-hour agencies with multiple terminals by:

1. Programmatic routing of all hit confirmation requests to a designated 24-hour terminal within the agency.
2. Programmatic routing, after hours of operations for the office where hit confirmation requests are normally received, to a designated 24-hour terminal within the agency.

INSTRUCTOR'S NOTE: THE NON-24-HOUR OFFICE MAY ELECT TO (1) PROVIDE COPIES OF THE CASE REPORTS/WARRANTS FOR ACTIVE NCIC RECORDS, (2) DESIGNATE A CONTACT PERSON FOR HIT CONFIRMATION, OR (3) INSTRUCT PERSONNEL AT THE 24-HOUR TERMINAL TO ACKNOWLEDGE A HIT CONFIRMATION REQUEST AND PROVIDE INFORMATION AS TO WHEN THE NON-24-HOUR OFFICE WILL RESPOND TO THE HIT CONFIRMATION REQUEST.

Hit confirmation coverage may be provided for non-24-hour terminal agencies by:

1. Programmatic routing of all hit confirmation requests to a designated 24-hour terminal within a 24-hour agency.

7/1/92

HC-10

2. Programmatic routing, after hours, of hit confirmation requests to a designated 24-hour terminal within a 24-hour agency.
3. Placing in the Miscellaneous Field of the NCIC record the telephone number or the ORI of a designated 24-hour agency responsible for hit confirmation requests.

INSTRUCTOR'S NOTE: THE NON-24-HOUR TERMINAL AGENCY MAY ELECT TO (1) PROVIDE COPIES OF THE CASE REPORTS/WARRANTS FOR ACTIVE NCIC RECORDS, (2) DESIGNATE A CONTACT PERSON FOR HIT CONFIRMATION, OR (3) INSTRUCT PERSONNEL AT THE 24-HOUR TERMINAL AGENCY TO ACKNOWLEDGE A HIT CONFIRMATION REQUEST AND PROVIDE INFORMATION AS TO WHEN THE NON-24-HOUR TERMINAL AGENCY WILL RESPOND TO THE HIT

CONFIRMATION REQUEST.

HD #5

Hit confirmation coverage may be provided for 24-hour nonterminal agencies by:

1. Programmatic routing of all hit confirmation requests to a designated 24-hour terminal within a 24-hour agency.
2. Placing in the Miscellaneous Field of the NCIC record the telephone number of the nonterminal agency.

INSTRUCTOR'S NOTE: THE 24-HOUR NONTERMINAL AGENCY MAY ELECT TO (1) PROVIDE COPIES OF THE CASE REPORTS/WARRANTS FOR ACTIVE NCIC RECORDS, (2) DESIGNATE A CONTACT PERSON FOR HIT CONFIRMATION, OR (3) INSTRUCT PERSONNEL AT THE 24-HOUR TERMINAL AGENCY TO ACKNOWLEDGE A HIT CONFIRMATION REQUEST AND PROVIDE INFORMATION AS TO WHEN THE 24-HOUR NONTERMINAL AGENCY WILL RESPOND TO THE HIT CONFIRMATION REQUEST.

Hit confirmation coverage may be provided for non-24-hour nonterminal agencies by:

1. Programmatic routing of all hit confirmation requests to a designated 24-hour terminal within a 24-hour agency.

7/1/92

HC-11

2. Placing in the Miscellaneous Field of the NCIC record the telephone number of the non-terminal agency and the telephone number of the designated 24-hour agency responsible for hit confirmation requests after hours.

INSTRUCTOR'S NOTE: THE NON-24-HOUR NONTERMINAL AGENCY MAY ELECT TO (1) PROVIDE COPIES OF THE CASE REPORTS/WARRANTS FOR ACTIVE NCIC RECORDS, (2) DESIGNATE A CONTACT PERSON FOR HIT CONFIRMATION, OR (3) INSTRUCT PERSONNEL AT THE 24-HOUR TERMINAL AGENCY TO ACKNOWLEDGE A HIT CONFIRMATION REQUEST AND PROVIDE INFORMATION AS TO WHEN THE NON-24-HOUR NONTERMINAL AGENCY WILL RESPOND TO THE HIT CONFIRMATION REQUEST.

The hit confirmation process described above is the minimum standard that has been established by NCIC. Your CTA or SC may have additional requirements. Consult your state operating manual or CTA for more information.

VII. PROBABLE CAUSE

IO #5

An NCIC hit is not probable cause to arrest or seize property. It is one factor which must be added to other facts and circumstances to have sufficient legal grounds for probable cause to arrest and seize property.

However, based on the decision in U.S. v. Hensley, 83 L.Ed.2d. 604 (1985), an NCIC hit would establish reasonable suspicion to detain an individual to briefly investigate the circumstances, including verifying and confirming the NCIC hit.

HD #6

7/1/92

HC-12

by

VIII. CONCLUSION

OH #6

Hit confirmation is the primary tool for ensuring that the proper person is apprehended or located and that the correct property is seized. It is particularly important to remember:

- A. Entering and inquiring agencies must follow the NCIC Ten-Minute Hit Confirmation policy.
- B. Hit confirmation documentation should be retained.
- C. Hit confirmation must be available 24 hours a day, 7 days a week, every day of the year.
- D. A hit alone is not probable cause to arrest.

Failure to follow the outlined hit confirmation policies could result ultimately in civil lawsuits and costly penalties for the criminal justice agency.

SHOW NCIC
VIDEO

BIBLIOGRAPHY

National Law Enforcement Telecommunications System, Inc., NLETS User Guide - New Version, February 8, 1991.

People Magazine, July, 1989 by Michael Neill, David Lustig in Hawthorne. "Roberto Hernandez Battles His Arresting Similarities to a Wanted Man with the Same Name."

Privacy Journal, April, 1987, Vol. XIII, NO. 6 " A Hit and an Error."

The State, October, 1987 by Bob Stuart. "Loss of FBI Computer Leaves a Void in Bambug County Law Enforcement."

U.S. Department of Justice. Federal Bureau of Investigation. "Areas of Liability" Terry Dean Rogan vs. City of Los Angeles Washington, D.C. Revised April, 1988.

U.S. Department of Justice. Federal Bureau of Investigation. "NCIC Hit Confirmation" Video. Washington, D.C.

U.S. Department of Justice. Federal Bureau of Investigation. National Crime Information Center Operating Manual Washington, D.C. May 31, 1989. Revision 55.

U.S. v. Hensley, 83 L.Ed.2d. 604 (1985).

The Washington Post, "Mistaken Identity Results in 18 Day Stay in D.C. Jail", by Douglas Stevenson. April, 1987

FBI/NCIC

HIT

CONFIRMATION

271

272

ROBERTO HERNANDEZ BATTLES
HIS ARRESTING SIMILARITIES
TO A WANTED MAN WITH
THE SAME NAME

MS. SMITH SETTLED HER
LAW SUIT AGAINST THE
SHERIFF'S DEPARTMENT

TERRY DEAN ROGAN
vs.
THE CITY OF LA

MISTAKEN IDENTITY RESULTS
IN 18 DAY STAY IN DC JAIL

CONFIRMING A HIT MEANS TO ENSURE:

Person/Property is Identical.

Warrant/Theft Report is Outstanding.

Decision Regarding Extradition/Return of Property.

YQ.(SNDORI000).(DSTORI000).TXT

HIT CONFIRMATION REQUEST-CONFIRM WITHIN 10 MINUTES

NIC/____.SYSTNO/____.REFNO____.OCA/____.

STOLEN VEHICLE - LIC/____.VIN/____.VYR/____.VMA/____.

WANTED PERSON - NAM/____.DOB/____.RAC/____.SEX/____.

MISSING PERSON - NAM/____.DOB/____.RAC/____.SEX/____.

STOLEN LICENSE - LIC/____.LIS/____.LIY/____.LIT/____.

STOLEN GUN - SER/____.CAL/____.MAK/____.MOD/____.

STOLEN ARTICLE - TYP/____.SER/____.BRA/____.

STOLEN SECURITY - TYP/____.SER/____.DEN/____.

STOLEN BOAT - REG/____.BHN/____.BMA/____.

STOLEN PART - SER/____.BRA/____.CAT/____.

REMARKS FROM LOCATING AGENCY:

PLEASE PROVIDE A SUBSTANTIVE RESPONSE WITHIN 10 MINUTES OR A NOTICE
OF THE SPECIFIC AMOUNT OF TIME NECESSARY TO CONFIRM OR REJECT
THIS HIT.

TNX AUTH _____

PHONE _____ ALT. PHONE _____

FAX AVAIL. _____ PHOTO AVAIL. _____

ANY CITY PD, OPR: _____ .TIME: _____

YR.(SNDORI000).(DSTORI000).T

HIT CONFIRMATION RESPONSE REFERENCE:

NIC/____.SYSTNO/____.REFNO/____.OCA/____.
STOLEN VEHICLE - LIC/____.VIN/____.VYR/____.VMA/____.
WANTED PERSON - NAM/____.DOB/____.RAC/____.SEX/____.
MISSING PERSON - NAM/____.DOB/____.RAC/____.SEX/____.
STOLEN LICENSE - LIC/____.LIS/____.LIY/____.LIT/____.
STOLEN GUN - SER/____.CAL/____.MAK/____.MOD/____.
STOLEN ARTICLE - TYP/____.SER/____.BRA/____.
STOLEN SECURITY - TYP/____.SER/____.DEN/____.
STOLEN BOAT - REG/____.BHN/____.BMA/____.
STOLEN PART - SER/____.BRA/____.CAT/____.
PHONE____ALT. PHONE____
FAX AVAIL.____PHOTO AVAIL.____
TNX AUTH_____

CONFIRMATION/EXTRADITION REMARKS FROM RESPONDING AGENCY:

-OR-

NOTICE OF SPECIFIC TIME AMOUNT NECESSARY TO CONFIRM OR REJECT
HIT:

ORI OF RECORD NEEDS _____
_____ TO CONFIRM OR REJECT HIT.

COURSE SUMMARY

- A. Entering and inquiring agencies must follow the NCIC ten-minute hit confirmation policy.
- B. Hit confirmation documentation should be retained.
- C. Hit confirmation must be available 24 hours a day, 7 days a week, every day of the year.
- D. A hit alone is not probable cause to arrest.

Mistaken Identity Results In 18-Day Stay in D.C. Jail

By Douglas Stevenson
Washington Post Staff Writer

187
John Edward Willis Jr., a 27-year-old computer operator, was arrested while waiting to cross a street near his Northwest home this month, fingerprinted and incarcerated for 18 days—until his fingerprints were taken again yesterday, proving that police had locked up the wrong man.

Willis, who claimed he was sexually assaulted while in custody, was released from D.C. Jail after his fingerprints were taken at the courthouse yesterday afternoon and

it became apparent that the prints did not match those of the man named on the Superior Court bench warrant, John H. Wills Jr. Willis is wanted for theft and unauthorized use of a vehicle.

"We determined today that he [Willis] was the wrong person by fingerprint process," Associate Judge Geoffrey Alprin said in a telephone interview, "and that's when I sent" the release order.

Willis was arrested by D.C. police at 15th and W. streets NW on the morning of Friday, April 10, taken to the 3rd District police station and held without bond at D.C. Jail

that weekend, he said in a joint interview with his lawyer, Shirlimarie Gray.

"I was going out to the bank," Willis said. "It was about 10 a.m. ... and the police stopped me. They said I looked like I was going to commit suicide."

"When they brought him in [to the station at 1620 V St. NW], supposedly they found this outstanding bench warrant for a person who had a similar name," Gray said.

Willis said police "had my I.D. ... That should have been enough for them. They saw my picture and everything, and they should have known who I was, but they didn't believe me."

According to the arrest book at the 3rd District cell block, John Willis, 27, of the 1400 block of W St. NW is listed as having been ar-

See LOCKUP, A27, Col. 1

Fingerprints End Jail Stay For Wrong Man

LOCKUP, From A1

rested April 10, in the 2100 block of W Street NW. The charges against Willis are listed as damage to property related to an outstanding warrant and "BRA," meaning a Bail Reform Act violation.

Gray said her client was charged at the station and taken to D.C. Superior Court for arraignment. But, once at the courthouse, it was decided that Willis would be held in D.C. Jail without bond pending a Monday, April 13, hearing before Judge Alprin, who issued the bench warrant for Willis.

At the April 13 hearing, Gray said she and her client were shown a copy of the indictment for Willis, listing "various charges" including unauthorized use of a vehicle and first-degree theft.

"My client indicated that he and Mr. Willis were not the same client," Gray said, and Alprin informed her that she needed to contact Willis' attorney. She said, "The judge set a surety bond on Mr. Willis, still believing him to be [Willis]," and Willis was transferred to the D.C. Jail.

Then Gray began the arduous process of investigating her client's claim. Willis' lawyer was contacted, the situation was explained, and Gray asked him to check with his client, she said.

She also asked him repeatedly to confirm her client's identity. "I really pressed this attorney to go to the jail."

Gray said she also checked the police identification numbers, issued when a person is arrested, and she found that the numbers differed. (Willis, Gray's client, had been arrested previously on a charge that was later dismissed, she said.)

The other attorney confirmed yesterday that Willis was not his client, Gray said, but meanwhile, according to Gray, Willis was the subject of harassment at the jail and was denied medication that had been prescribed for a neck injury. A neck brace was also taken away and has not been returned, Willis said.

Earlier, while in a lockup at the courthouse for his April 13 arraignment, Willis, handcuffed and manacled, was sexually assaulted and beaten by another prisoner, Willis and Gray said.

"His face was battered and quite bruised," Gray said, and she requested at the arraignment that Willis be held in isolation at the jail for his protection. Alprin included that stipulation on the commitment order, but Gray and Willis said that Willis was held in a general lockup area in the company of other prisoners.

Once Willis' identity was confirmed by the other attorney, Gray said, a second hearing before Judge Alprin was arranged.

At the 9 a.m. hearing yesterday, Alprin requested that the government confirm the identification in question and that assistant U.S. Attorney Robert Morgan be present as well, Gray said.

With Morgan and Gray in attendance, a government fingerprint man took Willis' prints in the lockup behind the courtroom at about 11:50 a.m., Gray said. "The fingerprint man, on the spot, told the government and myself that the fingerprints did not match the prints of one John H. Willis," the man listed on the warrant.

Morgan could not be reached for comment last night, but Gray said he and Alprin apologized, and Willis was ordered released.

Gray was told that her client would be released to her at 1 p.m. at the courthouse, but at 4:30 p.m., after repeated delays involving D.C. Jail personnel and U.S. Marshals Service officials (who said initially that Willis could not be released "because he had an 'AKA' or alias," Gray said), she was informed that Willis had been shipped back to the D.C. Jail. "I went berserk, to put it mildly," she said.

Gray asked Alprin to intervene again, and Willis was finally released at 5:40 p.m.

"The thing that troubles me—and I think it troubles the judge and Mr. Morgan—is, how did this happen?" Gray said.



Areas of Liability for the Criminal Justice Information System Administrator

Revised April, 1988



An area of concern to law enforcement officials and criminal justice information system administrators is the liability which is imposed on them for the overall operation and maintenance of a criminal justice information system. The management of the system brings forth a very large administrative responsibility. This responsibility is continuously reviewed and defined by the courts. The types of legal liability that may result from the maintenance and dissemination of criminal justice data will be reviewed in this paper to provide insight to the administrator.

In discussing actions which might be maintained against a criminal justice agency employee for "record malpractice," a look at immunity and one's status will first be reviewed. Under the principle of sovereign immunity, the United States or any state therein cannot be sued by reason of their sovereignty. However, suits may be entertained by the United States, if specific permission has been granted by an act of Congress. An example of this is the Federal Tort Claims Act, 28 United States Code 2671, et. seq., which makes the United States liable for the negligent acts or omissions of Federal employees within the scope of their employment. Most states possess some kind of system which permits them to assume liability and allows civil suits against them also. This is normally provided via constitutional or statutory authority.

The move away from immunity and toward responsibility has taken different forms. Even though a state may have

immunity and its agencies are protected from suit, its officials and employees are not protected in their capacities under the doctrine of sovereign immunity. However, there are two types of official immunity: (1) absolute immunity, and (2) qualified immunity. In an action for a common law tort, absolute immunity from suit is granted to a government official when that official performs a discretionary act within the scope of his authority, even if this act is performed with malice. Discretionary acts are basically high-level policy and planning decisions. In theory, the operation of the government depends upon its ability to make decisions on the highest level, which decisions should be free of nuisance litigation. Ministerial acts, on the other hand, are day-to-day acts of the government which carry out the decisions made on the discretionary level. Ministerial acts, which implement policy decisions, are subject to liability while discretionary acts are immune to suit. Qualified immunity is generally applicable to lower ranking officials in performing ministerial acts.

Generally, absolute immunity is not available to Federal officials as a defense in suits alleging constitutional violations, subject to those exceptional situations where it is demonstrated that absolute immunity is essential for the conduct of public business; actions of presidents, judges, and prosecutors. However, in the area of constitutional torts, the U. S. Supreme Court has recently advanced a change. In a series of opinions, the U. S. Supreme Court has ruled that government officials involved in a wide range of executive decision-making and police functions have qualified immunity

to actions for damages charging them with violations of civil rights. Note that the distinction between discretionary acts and ministerial acts is not an issue in these types of cases. Under the earlier opinions, these officials could avoid liability for a constitutional violation if they proved (1) that they held a good faith belief that their actions were lawful and (2) that this belief was objectively reasonable given the state of the law at that time. Procunier v. Navarette, 434 U.S. 555 (1978) (prison officials); Wood v. Strickland, 420 U.S. 308 (1975) (school board members); O'Connor v. Donaldson, 422 U.S. 563 (1975) (mental hospital officials); Butz v. Economou, 438 U.S. 478 (1978) (Federal government cabinet level officers); Scheuer v. Rhodes, 416 U.S. 232 (1974) (state executive officials); Pierson v. Ray, 386 U.S. 547 (1967) (police officers).

These cases had provided a framework for litigating the qualified immunity defense. The defendant was generally believed to bear the burden of pleading and proving at trial that the constitutional right at issue was not clearly established at the time of the incident and that he did not maliciously intend to cause a deprivation of constitutional rights or other injury to plaintiff, Wood v. Strickland, supra, at 321-22; Procunier v. Navarette, supra. These standards, of course, were not always easy to apply and resolution of the immunity issue has proved quite complex in some situations.

In Harlow v. Fitzgerald, 457 U.S. 800 (1982), the Court reconsidered the doctrine of qualified immunity and announced a fundamental change in its scope and application. In an attempt to allow for pretrial adjudication of the qualified immunity issue, the Court appeared to discard the subjective element of good faith, focusing instead on the state of the law at the time of the alleged constitutional violation. The Court ruled:

Consistently with the balance at which we aimed in Butz, we conclude today that bare allegations of malice should not suffice to

subject government officials either to the costs of trial or to the burdens of broad-reaching discovery. We therefore hold that government officials performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known. See Procunier v. Navarette, 434 U.S. 555, 565 (1978); Wood v. Strickland, supra, 420 U.S. at 321.

Reliance on the objective reasonableness of an official's conduct, as measured by reference to clearly established law, should avoid excessive disruption of government and permit the resolution of many insubstantial claims on summary judgment. On summary judgment, the judge appropriately may determine, not only the currently applicable law, but whether that law was clearly established at the time an action occurred. If the law at that time was not clearly established, an official could not reasonably be expected to anticipate subsequent legal developments, nor could he fairly be said to "know" that the law forbade conduct not previously identified as unlawful. Until this threshold immunity question is resolved, discovery should not be allowed. If the law was clearly established, the immunity defense ordinarily should fail, since a reasonably competent public official should know the law governing his conduct. Nevertheless, if the official pleading the defense claims extraordinary circumstances and can prove that he neither knew nor should have known of the relevant legal standard, the defense should be sustained. But again, the defense would turn primarily on objective factors (footnotes omitted).

Litigation of the good faith defense after Harlow has revolved around the difficult questions raised by the term "clearly established law." The principle announced in Wood v. Strickland,

supra, that defendants could not, as a matter of law, avoid liability where the rights were clearly established, is not diluted by Harlow. As the Court stated in Wood, at 321-22:

The official himself must be acting sincerely and with a belief that he is doing right, but an act violating a student's constitutional rights can be no more justified by ignorance or disregard of settled, indisputable law on the part of one entrusted with supervision of students' lives than by the presence of actual malice.

Therefore, in the specific context of school discipline, we hold that a school board member is not immune from liability for damages under §1983 if he knew or reasonably should have known that the action he took within his sphere of official responsibility would violate the constitutional rights of the student affected....

The qualified immunity from liability based on good faith is applicable to both state and Federal law enforcement officials. Pierson v. Ray, supra; Bivens v. Six Unknown Named Agents, 456 F.2d 1339 (2d Cir. 1972); Barker v. Norman, 651 F.2d 1107 (5th Cir. 1981); Boscarino v. Nelson, 518 F.2d 879 (7th Cir. 1975). However, given the wide variety of constitutional torts which may be at issue in police misconduct litigation, one cannot expect the definition of good faith that was developed with respect to government officials, who execute functions quite different from those of police officers, to provide a satisfactory test for every police misconduct case. Indeed, the current tendency of the courts to mechanically apply the general good faith defense to all aspects of police work has led to confusion and doctrinally incorrect decisions in the lower Federal courts. Procunier v. Navarette, supra, at 568 (Steven, J., dissenting).

To illustrate how courts have looked at the question of discretionary acts, the case of Walcowski v.

Macomb County Sheriff, 236 Northwest 2d 516 (1975) should prove to be informative. The plaintiff was stopped for running a red light by officers of the defendant. A check was made of the Michigan State Police Department's Law Enforcement Information Network (LEIN) which indicated an outstanding warrant on the plaintiff for perjury, a felony. This was an error even though the plaintiff was wanted on a contempt of court cite, a misdemeanor. The plaintiff contended that if the officers had been correctly informed that there was a "misdemeanor want" as opposed to a "felony want," the officers would not have taken the plaintiff into custody. The plaintiff sued for battery, assault, false arrest, unlawful imprisonment, and defamation. The defendant, Director of the Michigan State Police Department, who maintained the computer service, appealed in this case from the lower court's refusal to drop him from the action. The court held that the "operation of police departments are governmental functions within the meaning of the statute," Michigan Statutes, Section 3.996(107), "which provides immunity from tort liability to governmental functions. Therefore, the activities of the director in overseeing the operations of a computerized criminal record system are discretionary, and he was therefore immune from this suit by operation of state law."

It can be said that the policy decision areas, i.e., planning, overseeing, and running a criminal justice information system is the exercising of discretionary acts. However, other cases have dealt specifically with the issue of what is the "scope of authority" of the government official and to what extent there can be an abuse of the same. The case of Maney v. Ratcliff, 399 F. Supp. 760 (1975), discusses this issue. The plaintiff brought the instant action against certain Louisiana law enforcement officials based on a cause of action arising under the Federal Civil Rights Law (42 United States Code 1983) challenging the manner which the defendants had used the NCIC System to locate the plaintiff. The plaintiff was

arrested on three separate occasions on the basis of an NCIC entry indicating that he was wanted by authorities on a felony narcotics charge. The plaintiff was not extradited and the NCIC entry was never cleared. The Court stated "although the decision of whether to extradite is within the 'quasi-judicial' function of a state prosecutor, conduct of the Louisiana District Attorney's Office in leaving the outstanding arrest warrant entry on the FBI NCIC computer system, after having decided not to extradite the plaintiff, was not within the prosecutorial function and was outside the scope of prosecutorial immunity in a civil rights suit." Thus, the immunity which the prosecutor would normally have as a government official did not extend to an act beyond the prosecutor's scope of authority, i.e., allowing the entry to remain on file. Additionally, an issue in the Maney case was the plaintiff's alleged violation of Fourth Amendment rights. As indicated previously, the suit was being maintained under the civil rights statute, and in order to maintain this type of litigation a case must allege a deprivation of a right, privilege, or immunity which is secured by the Constitution. This alleged deprivation must be caused by a person acting under color of state law. The Maney Court found the complaint sufficient to state a cause of action for violation of the plaintiff's Fourth Amendment rights. The Court held that, under the facts as presented, although the failure to take the entry out of the NCIC computer after the first arrest did not constitute an unreasonable search and seizure, the failure to delete after the second arrest "evinced a reckless and careless disregard for the plaintiff's constitutional rights."

Harlow v. Fitzgerald, supra, makes it clear that a threshold determination in all cases in which defendants plead qualified immunity is whether the government officer was performing a "discretionary function." Barker v. Norman, 651 F.2d 1107 (5th Cir. 1981); Williams v. Treen, 671 F.2d 892 (5th Cir. 1982). Police officers and prison guards do not as a rule exercise the kind

or scope of discretionary judgment exercised, for example, by presidential assistants (Harlow) or governors (Scheuer v. Rhodes, 416 U. S. 232 (1974)). Moreover, given the wide range of actions undertaken by police officers, it is not unreasonable to expect that there will be distinct differences between types of police work in terms of whether discretionary or ministerial duties are involved. Accordingly, an initial burden should be placed on the officer to demonstrate that the particular authority exercised in the case was discretionary in nature. Williams v. Treen, supra.

There are a number of situations under which a police officer who has violated someone's constitutional rights will assert a good faith defense. Easiest to analyze is the one in which an officer acts pursuant to a statute reasonably believed to be valid but later declared unconstitutional. Given the Supreme Court's rulings on the good faith defense, the officer's strongest case for reliance upon legal authority for his unconstitutional actions arises when his actions are sanctioned by a statute. Pierson v. Ray, supra, at 555.

Similarly, where the officer has in good faith secured or executed a search warrant, or has followed other court orders, he or she will normally be protected even if the warrant or order is invalid. Smith v. Martin, 542 F.2d 688 (6th Cir. 1976); Stadium Films, Inc. v. Baillargeon, 542 F.2d 577 (1st Cir. 1976). However, in McSurely v. McClellan, 697 F.2d 309 (D.C. Cir. 1982), modified on other grounds, 753 F.2d 88 (D.C. Cir. 1985), the court ruled that a prosecutor can be held liable for a search conducted pursuant to warrant if there was fraud in the procurement of the warrant or if the prosecutor should have known that the warrant was illegal or should not have been issued.

Similarly, in Briggs v. Malley, 106 U. S. 1092 (1986), the U.S. Supreme Court concluded that a law enforcement officer is entitled only to qualified, not absolute, immunity from liability in a civil rights action based on a claim that the officer caused an

unconstitutional arrest by obtaining a warrant on the basis of a complaint and affidavit that were insufficient to establish probable cause; qualified immunity is not established simply by virtue of the fact that the officer believed the allegations in the affidavit and that a judicial officer found the affidavit sufficient. In Briggs v. Malley, the Court stated that, as a matter of public policy, qualified immunity provides ample protection to all but the plainly incompetent or those who knowingly violate the law.

As to constitutional issues which continue to be raised with reference to maintenance of inaccurate or incomplete records, one needs to review the case of the United States v. Mackey, 387 Fed. Supp. 1121 (1975). In this case, the plaintiff was hitchhiking when he was approached and stopped by two police officers who made a routine NCIC check. The officers were advised that there was an outstanding fugitive warrant on the subject, and they arrested him, which they would not have done otherwise. While processing the plaintiff, an unregistered shotgun was found in a dufflebag. The plaintiff was indicted on a Federal firearms charge. Subsequently, it was determined that the fugitive warrant actually had been satisfied five months earlier, but had not been removed from the NCIC System. The plaintiff made a motion to suppress the shotgun as evidence on the basis that his arrest, which was made pursuant to an incorrect NCIC arrest warrant entry, was illegal and constituted a denial of due process under the Federal Constitution. The Court held the evidence inadmissible and that the plaintiff's arrest was equivalent to an arbitrary arrest and was actually a denial of due process. The Court stated "that a computer inaccuracy of this nature and duration, even if unintended, amounted to a capricious disregard for the rights of the defendant as a citizen of the United States. The evidence compels a finding that the Government's action was equivalent to an arbitrary arrest and that an arrest on this basis deprived the defendant of his liberty without due process of law. Once the warrant was satisfied, five months before the

defendant's arrest, there no longer existed any basis for his detention and the Government may not now profit by its own lack of responsibility." It might be pointed out that in the Mackey case, the decision was made by the Court without attempting to determine the actual responsibility for the NCIC error but that this stale information did constitute an infringement of the plaintiff's rights and that this infringement was "perpetrated primarily with the assistance of a mindless automation controlled by the Government." It should be noted that in the Mackey case, the Judge mistakenly referred to an NCIC inquiry, when in fact, the inquiry and record were in the California system. However, this does not alter the basic ruling of the Court as it applies to possible liability because of state records in a computerized system.

Having looked at areas of liability with respect to immunity and subsequently constitutional areas that have been the subject of challenges involving computerized information, we now move to a third area. This area will be a discussion of the criminal justice agency's obligation to maintain accurate information. Of significant interest in this area is the case of Tarlton v. Saxbe, 507 F.2d 1116 (1974). In this case, the plaintiff's FBI criminal record contained a number of arrests without dispositions. The plaintiff wanted these records expunged from his file. His action was dismissed in the lower court and he appealed that dismissal. On appeal, the question which was reviewed by the court was "what type of duty does the FBI have in safeguarding the accuracy of information which it has in its criminal files which can subsequently be disseminated." The court said that the FBI has "some duty" to ensure that the records which it maintains and disseminates are reasonably accurate.

It also stated that the "primary duty" for accuracy of a record is placed on the local agency who makes the arrest or conviction rather than the FBI. The court did reject the argument offered by the Government of the "passive recipient" theory in that the FBI is a mere repository for information

collected and recorded by state and local agencies and thus is not responsible for any inaccuracies in that information. It should be pointed out that the Tarlton case specifically reviewed the duty of the FBI and not specifically the type of duty which would be imposed on a criminal justice agency for ensuring the accuracy of its records.

However, subsequent to Tarlton, the case of Testa v. Winquist, 451 F.Supp. 388 (1978) tends to shed some light on negligent record keeping as forming a basis for personal liability of local officials. [Although the decision is somewhat complex, it is especially relevant because it involves damage claims based on alleged deprivations of constitutional rights as well as on common law tort theories. It also involves issues of primary as well as contributory negligence resulting from record-keeping practices.] In Testa, the plaintiffs were detained overnight by East Providence, Rhode Island, police officers and charged with possession of a stolen car based on information supplied by the NCIC, and confirmed by telephone by a Warwick, Rhode Island, police officer indicating that the car the plaintiffs were driving was stolen. In fact, the car had previously been stolen in Warwick but had been recovered and subsequently sold to the plaintiffs.

The plaintiffs brought a civil damage action against the East Providence police officers for deprivation of constitutional rights (false imprisonment), pursuant to 42 USC 1983, and for state tort claims, including false imprisonment, libel and slander, trespass, and malicious destruction of property. The police officers joined the regional administrator of NCIC and the Warwick police officer as third party defendants on the grounds that these individuals had negligently failed to keep current and accurate records and had supplied erroneous information on which the police officers had relied to their detriment. Thus, if the police officers were found liable to the plaintiffs, the third party defendants should bear or share this liability under state theories of contribution and indemnity.

The third party defendants moved to dismiss the claim against them and the court denied the motion, it concluded that under the facts alleged, the defendant police officers could be found to be liable to the plaintiffs and the third party defendants could be required to share this liability because of their negligent record-keeping practices. In discussing the liability of the defendant police officers, the court said that although the officers were performing discretionary duties and were entitled to a defense of qualified immunity, this immunity could be overcome by showing that they had unreasonably relied on the NCIC computer check and the Warwick police officers' confirmation as the sole basis for probable cause to detain the plaintiffs. Citing Bryan v. Jones, 530 F.2d 1210 (1976), the court said that, in Section 1983 suits for false arrest and imprisonment, the defense of qualified immunity has a reasonableness component. The police officers must show not only that their acts were nonmalicious, but also that they acted reasonably under the circumstances. If they negligently relied solely on the computer check and telephone confirmation without making further pertinent inquiries, they could be held liable. The court also ruled that the NCIC administrator and the Warwick police officer could be held jointly or severally liable for breach of a duty owed to the plaintiffs to maintain accurate and current record systems. Since it is commonplace for arresting officers to rely heavily on computer checks and police department record systems, the persons who maintain these systems have a duty to establish reasonable administrative mechanisms designed to minimize the risk of inaccuracy by requiring that the records be constantly updated. Where breach of this duty results in illegal arrest, the arrestee may have a cause of action for false arrest actionable under both state and Federal law.

The court, in discussing the various duties which should have been imposed on the administrator of the information system, indicates that a duty with respect to the maintenance of individual

criminal history record information has been established by statute, 42 United State Code, Section 3771(b). This subsection, amended in 1984, now located at 42 U.S.C. 3789g (b), deals with criminal history information disposition and arrest data and states:

"All criminal history information collected, stored, or disseminated through support under this chapter shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included therein. The collection, storage, and dissemination of such information shall take place under procedures reasonably designed to ensure that all such information is kept current therein; the Office of Justice Programs shall assure that the security and privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes. In addition, an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this chapter, shall, upon satisfactory verification of his identity, be entitled to review such information and to obtain a copy of it for the purpose of challenge or correction."

This Section at Subsection (d) also imposes a sanction which provides that "any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed \$10,000, in addition to any other penalty imposed by law."

It appears from the cases that have been cited, the courts have now specifically addressed the issue as to whether a criminal justice information system administrator can be held liable for the negligent mishandling of a criminal justice record. We can see that, in relation to 42 United State Code 3789g, there is a standard which is prescribed for record management and perhaps the establishment of maintenance standards for these records.

It can be said that criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up to date. To ensure that legally sufficient record management is present, each administrator should ensure that there are security standards, audit standards, and personnel training standards which would allow accurate and up-to-date records and dissemination of the same.

In addition to the liability that may be imposed on an NCIC Control Terminal Officer for maintaining inaccurate or stale information, etc., in the System, the question of the liability of an agency which totally fails to utilize the System, and this failure thereby results in harm to a third party, has been posed. This type of "failure to act" could be termed as nonfeasance. Nonfeasance is defined as the "nonperformance of some act which should be performed, omission to perform a required duty at all or total neglect of duty." (Black's Law Dictionary, revised fourth edition, West Publishing Company.)

When looking at the liability of law enforcement officers with respect to their specific failure to act, one must consider the "neglect of duty issue." The general rule is that police officers owe protection to the public and not specifically to any particular individual. In most police agencies, there are specific guidelines which establish and outline the nature and responsibilities of the office or officer. To be considered in violation of these duties or willfully neglecting one's duty, the officer must be aware of the nature and responsibilities of his office. Once the officer is placed on notice of his duties, he can possibly be held liable for intentionally omitting, neglecting, or refusing to carry out these duties. For example, if there are agency rules which require that a fugitive must be entered into a state or national system and the officer fails to enter the subject, and, thereafter, harm occurs to a third party, the officer may be held liable for his negligent conduct. As to specific cases involving the nonuse of a computer information system and nonfeasance on the part of a police agency, no specific cases were noted. However, in dealing

with the "neglect of duty" issue, the most widely recognized duty of a law enforcement officer is that of requiring him to avoid negligence in his work. Society has repeatedly imposed a duty upon individuals to conduct their affairs in a manner which would avoid subjecting others to unreasonable risk of harm. This, of course, applies to law enforcement officers. If the officer's conduct creates a danger recognizable as such by him in similar circumstances, he will be held accountable to others injured as a proximate result of his conduct and who have not contributed to their own harm. These general principles are well known concepts in the law of negligence. The tort of negligence is defined as "the omission to do something which a reasonable man, guided by those ordinary considerations which ordinarily regulate human affairs, would do, or the doing of something which a reasonable and prudent man would not do." (Black's Law Dictionary, revised fourth edition, West Publishing Company.)

This could be interpreted that actions taken by a police officer in investigations and/or the apprehension of criminals must not create an unreasonable risk of injury or death to innocent persons. This creation of the risk is not in and of itself negligence; however, the law does require reasonable assessments of the likelihood of harm and will regard as negligent any act which creates a risk of such magnitude as to outweigh the utility of the act itself. Restatement (Second) of Torts §291.

Under the civil courts system, if the police officer owes no specific duty to the complainant, he will not be penalized even if the plaintiff in fact suffered some form of injury. An officer will be liable anywhere it is shown that (1) he was obliged to do or refrain from doing something and (2) the plaintiff was damaged because of the officer's failure to comply with the particular obligation or duty to train officers they employ. Administrators have been held liable where there has been a negligent breach of this duty which approximately caused an injury to the plaintiff. The negligent failure to

train involves a breach of executive duty and imposes the same liability as if the administrator had participated in the actual tort. An example of this would be where a training officer fails to properly and diligently train his personnel in the proper use of the system, so as to allow them to carry out their required duties. Generally, a police administrator is not vicariously liable for the acts of the subordinate officer unless he participates in, directs, authorizes, or ratifies the misconduct of the officer. These usually involve some affirmative act by a police chief. A parallel could be drawn by looking at the case of Roberts v. Williams, 302 F. Supp. 972 (1969) where a county farm superintendent was held liable for the grossly negligent shooting of a county prisoner by an armed trustee. The trustee was furnished a loaded shotgun without training. The court held that "since the shooting in this case occurred under the most needless and avoidable circumstances, it is patent that Williams, the trustee, was thoroughly ignorant, indeed incompetent, in the handling of a firearm." The court went on to say that it was the superintendent's "duty to exercise care that Williams knew how to use the gun and could handle it safely before giving him possession of it." The negligence of the superintendent in this case combined with the negligence of Williams in mishandling the gun, produced a classic case of causation which approximately resulted in the shooting of and personal injuries to the plaintiff. It is no answer to say that Williams alone is responsible for the consequences of this negligence, but that responsibility must be shared by the superintendent because of his concurrent, tortious conduct.

More recently, in Monell v. New York City Department of Social Services, 436 U.S. 658 (1978), the Supreme Court held that municipalities are persons subject to damages and liability under 42 USC Section 1983, for violations of that act visited by municipal officials. The Court noted, however that municipal liability could not be premised on the mere fact that the municipality employed the offending official. Instead, the Court held that

municipal liability could only be imposed for injuries inflicted pursuant to government "policy or custom." The Supreme Court on June 3, 1985, in the case of City of Oklahoma City v. Tuttle, 105 U.S. 2427 (1985), clarifies Monell and indicates that where municipal liability is alleged and based on a policy of inadequate training, there must be a causal connection between the policy and the constitutional deprivation, that is there must at least be an affirmative link between the training inadequacies alleged and the particular constitutional violation at issue. These two cases are illustrative of the point that liability for inadequate training, resulting in mishandling criminal and other records, is a possibility.

Even more recent is the case of Terry Dean Rogan v. City of Los Angeles, Et. Al., No. CV 85-0989 (C.D. Cal. July 16, 1987). During 1981, using false identification in the name of Terry Dean Rogan, Bernard McKandes, an Alabama state prison escapee, was arrested and later released by the Los Angeles Police Department (LAPD) on suspicion of murder. In April, 1982, LAPD officer Richard Crotsley obtained a warrant in Rogan's name, charging him with two robbery-murders. The warrant contained an alias, but none of McKandes' known physical characteristics. In May of 1982, LAPD officer Lester Slack had the warrant information entered into the NCIC Computer System (without McKandes' known physical characteristics). In July of 1982, Slack reentered the record without modification.

Sometime around November, 1982, Rogan was arrested in Michigan for resisting arrest during a trespassing dispute. An NCIC check revealed the outstanding California arrest warrant. After comparing physical characteristics, it was determined that Rogan was not the same individual named in the warrant. The warrant was automatically removed from NCIC. However, in November of 1982, Crotsley had the record reentered without modification.

During 1983 and 1984, Rogan was arrested four times based on the warrant information contained in the NCIC System. Also, in July of 1983, Crotsley again reactivated the record in Rogan's name without modification. Finally, in January of 1984, after McKandes was returned to an Alabama prison, Crotsley removed the NCIC record in Rogan's name.

Rogan, in U.S. District Court, sued the City of Los Angeles and both LAPD officers under Title 42 U.S.C. Section 1983 for damages and other relief, alleging a deprivation of his constitutional rights because of his mistaken arrests.

On cross motions for summary judgment, the Court found the City of Los Angeles to be liable, but did not find liability on the part of the officers.

1) Inasmuch as descriptive data was available but not entered, the Court determined that the NCIC record and the arrest warrant upon which it was based violated the particular description requirement of the Fourth Amendment. The principle that the inadequacy of description in an arrest warrant so as to make it lack specificity making it unconstitutional was extended to the NCIC record.

2) The Court found that the maintenance and multiple reentry of the NCIC record without modification caused Rogan to be arrested and detained without due process of law. The officers stated they did not know how to change the NCIC record. The failure of the City of Los Angeles to train its officers in the use of NCIC and, therefore, the failure to enter other descriptive data when available in spite of NCIC established standards of training was gross negligence per se. Therefore, the City of Los Angeles was liable under Section 1983.

3) The Court held that the officers had qualified immunity this time because their conduct and omissions did not violate Rogan's clearly established constitutional rights of which a reasonable person

would have known. They did not know that the constitutional test of specificity in warrants applied to NCIC entries.

This decision represents a warning that the courts will not tolerate incomplete NCIC records nor the failure to train or provide adequate training in the proper use of the NCIC System. If that occurs, liability will be assessed at the appropriate and responsible levels of government.

In summation, with reference to the total nonuse of criminal justice information systems, there is no case law authority which specifically states that a system of this nature must be utilized by law enforcement agencies. This topic did not encompass all state statutory authority which might require utilization. However, it can be inferred that (1) negligent nonuse by a law enforcement officer when required by policy to utilize the system or (2) inadequate training by an administrator of an officer who must use the system pursuant to policy, may result in a finding by a court that breach of a specific duty has occurred and the persons involved are liable for damages under the general principles of tort law. Furthermore, based on Rogan, liability for a constitutional tort under Section 1983 may also result.

In closing, it should be pointed out that although the risk of personal liability appears not to be great, it is growing and the potential for liability clearly does exist. Therefore, it is important for criminal justice officials to understand the theories and boundaries of liability for record mishandling and to monitor court decisions that affect the scope of personal exposure of criminal record personnel.

NCIC

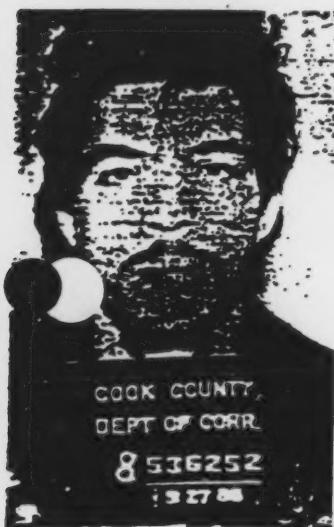
(NCIC)
**National
Crime
Information
Center**

ROBERTO HERNANDEZ BATTLES HIS ARRESTING SIMILARITIES TO A WANTED MAN WITH THE SAME NAME

TROUBLE

Roberto Hernandez admits he was driving drunk on Feb. 24, 1986, when police in Inglewood, Calif., pulled him over. He also admits that he had an outstanding traffic ticket when he was picked up in Hawthorne, Calif., on March 15, 1988. He insists, however, that he has never, ever, been in Chicago and that he most certainly did not try to break into a house there in 1985. It's his malign shadow, the other Roberto Hernandez—the Midwestern Roberto Hernandez—who's wanted for that. In the meantime, the West Coast Roberto Hernandez keeps getting arrested for a crime he didn't commit, in a city he has never visited.

The *Twilight Zone* troubles of Roberto Perales Her-



"This is a great country," says Hernandez, right, "but I can't get ahead if I keep going to jail" for a crime for which his namesake, left, is wanted.



TROUBLE

andez began, unbeknownst to him, on Sept. 25, 1985, in Chicago, when police there arrested a man named Roberto Hernandez as he was allegedly in the act of breaking into a house. Authorities say that Hernandez posted \$2,500 bail—and has not been seen since. Chicago police issued a warrant for him and routinely listed him in the national crime computer. They described him as follows: "5'8" tall, brown hair, tattoo on left arm, 160 pounds. Born Feb. 2, 1953."

The Hernandez who was wanted is not known to have a middle name, but he matches the identity of his unfortunate namesake in Los Angeles almost exactly.

Both men were born on Feb. 2, 1958. Both have tattoos on the left arm. And, except for one digit, their Social Security numbers are identical.

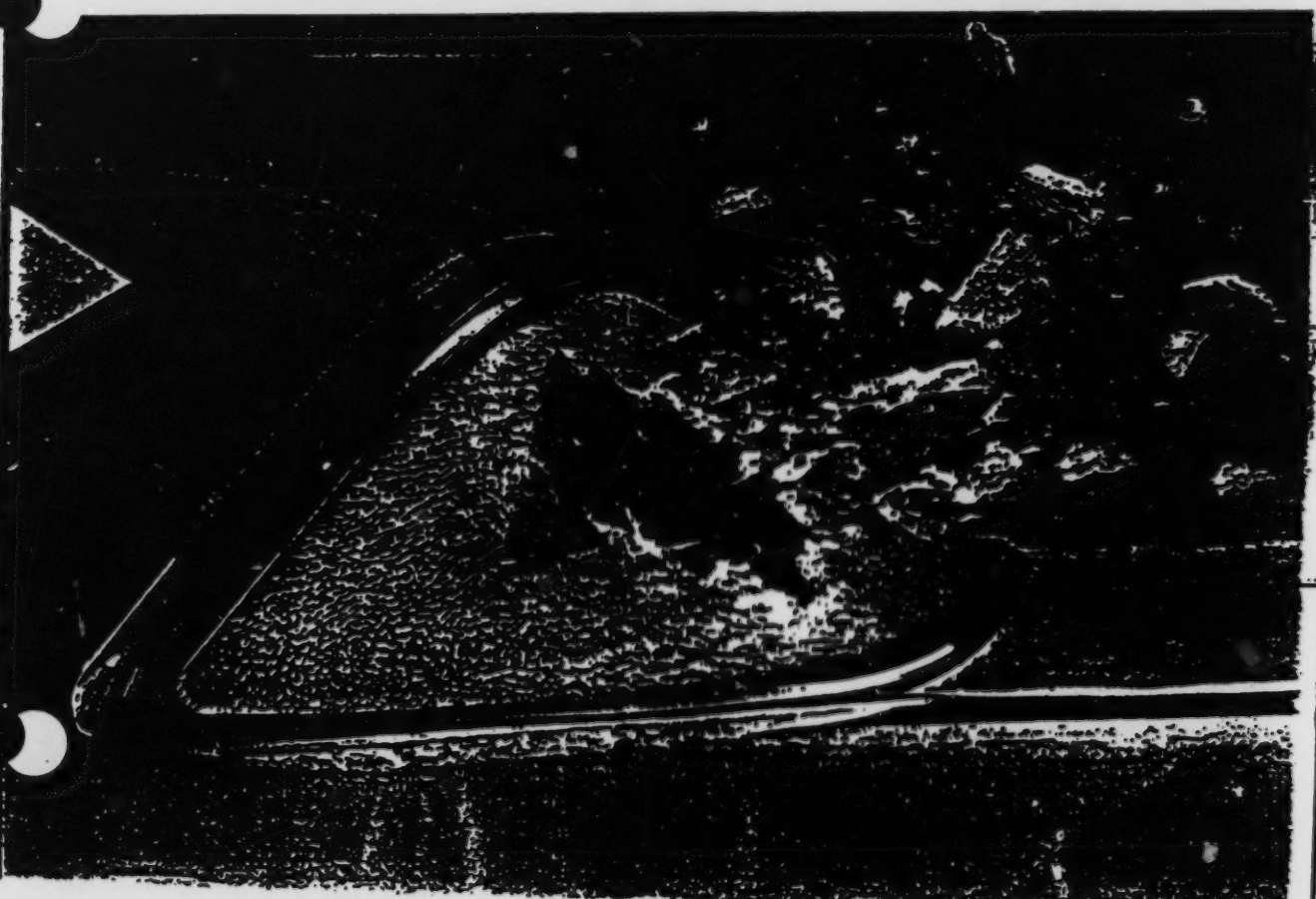
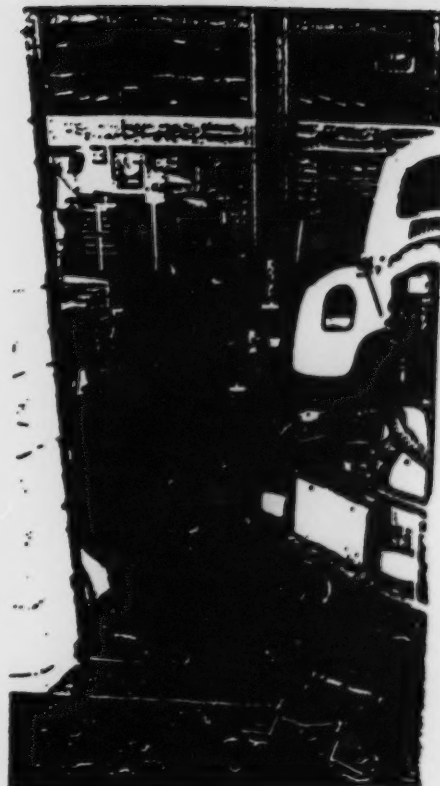
Naturally, Roberto Perales Hernandez was unaware of all this as he drove home on that February day three years ago to the one-bedroom apartment in Inglewood, where he lives with his wife, Alicia, 27, and their two children. An undocumented alien from Mexico who had been

in the United States since 1976, he had been looking for work as an auto mechanic. That morning, he had finally landed a job. On the way home he stopped for a few beers. Police spotted his car weaving in traffic and pulled him over. When he failed an alcohol-level test, he was handcuffed and taken to a police station, where he spent the night.

The next morning, before going to court on the drunken-driving charge, Hernandez was told by a deputy sheriff that he was wanted on a fugitive warrant from Chicago. "I've never been to Chicago," Hernandez remembers telling the officer. "I've never been east of Las Vegas." Hernandez says the deputy's response was curt: "That's what they all say."

Although he told his story to a lawyer from the public defender's office, Hernandez says he was put in the Los Angeles County Jail for 11 days pending transfer to Chicago. "They wanted me to sign extradition papers to send me back to Illinois," he says. "No way."

"When I see a police car," says Hernandez, at work, "I'm afraid I'll be stopped and the nightmare will start all over."





Finally, on March 7, Hernandez was released. "I went home and figured everything was behind me," he says. Because of the time spent in jail, Hernandez had lost the mechanic's job. A few weeks later, though, his public defender told him the county, although not admitting any responsibility for his ordeal, was of-

"I've never been to Chicago," Hernandez told the policeman. The gist of the officer's reply, as Roberto remembers it: "That's what they all say."

fering him \$7,000. He took the money. After being sentenced to three years' probation and mandatory AA attendance for the DUI arrest, Hernandez figured his troubles with the law were over.

Two years later, however, the other Roberto Hernandez burst into his life again. Roberto Perales Hernandez—by then working as a school bus mechanic—was driving his sister-in-law's car in Haw-

thorne. "I was still on probation and trying to behave," he says. "I didn't want any trouble from anyone." Unfortunately for him, the car carried an outdated registration sticker, and he was pulled over. When police ran his name through the computer, they came up with two warrants. One was for an unpaid traffic ticket. The other was for the Chicago burglary. This time, Hernandez was handcuffed and taken to the police station.

"I'm back at the police station," he says. "I call my wife. She comes down with the \$18 [for the old traffic ticket]. They say: 'I'm sorry. He's wanted in Chicago for robbery.'" This time, Hernandez spent a week in jail before being released. And this time, for a change, he kept his job.

But Roberto Perales Hernandez is angry. He is suing the city, county and state for the second arrest, charging false imprisonment, deprivation of civil rights and—not surprisingly—the infliction of emotional distress.

He hopes that Chicago police catch up with the other Roberto Hernandez.

And, in the meantime, he is driving very, very carefully.

—Michael Neill,
David Lustig in Hawthorne





PRIVACY JOURNAL

P.O. Box 15300
Washington, D.C. 20003
(202) 547-2865

an independent monthly on privacy in a computer age

April 1987, Vol. XIII, No. 6

A HIT AND AN ERROR

A New Jersey woman was strip searched and then jailed for eight days in 1983 on the basis of a National Crime Information Center computerized report that indicated a woman with the same name and birth date was wanted for welfare fraud in Dallas. The victim, Elaine Smith, had been stopped on a traffic violation. The target in Texas had a different Social Security number, middle initial, and physical description, but none of this information was recorded in the NCIC entry, as it is supposed to be.

As a result of the same erroneous computer "hit," Smith was detained for three days one month later. She was taken "screaming and hysterical" from her place of employment. For damages of \$15,000, the woman has now settled her lawsuit against the sheriff's department that relied on the report and the one in Texas that originated it. Smith v. County of Morris, 85-3417(JWB) (D.N.J. Mar. 16, 1987)

Research getting detail's

Copyright 1987 © Robert Ellis Smith
ISSN 0145-7659

Loss of FBI computer leaves a void in Bamberg County law enforcement

By BOB STUART
Orangeburg Bureau

BAMBERG

Bamberg County law enforcement officials say they've lost a valuable tool since the county was denied access to the FBI's national crime information computer six weeks ago.

"We can't enter information about stolen merchandise, weapons, criminals or lost persons in the FBI computer," Bamberg County Sheriff Ed Darnell said Thursday.

Darnell said a county man recently charged with criminal sexual conduct is at large, but without FBI computer access, he cannot notify authorities in other states.

The county's failure to meet state and federal guidelines was cited Oct. 1 when the State Law Enforcement Division informed Bamberg County it could no longer enter data through the

FBI computer.

Those guidelines require that the county teletype be monitored 24 hours a day, seven days a week by a licensed dispatcher, said SLED spokesman Hugh Munn.

Munn also said that Bamberg became the state's only county unable to enter information into the FBI computer. It can monitor information in the computer from other places.

Bamberg Mayor Virgil Hlicks said SLED had warned county government officials about the problem for the past year.

The teletype, which is housed at the Bamberg City Police Department, is monitored continually by three city dispatchers from 5 p.m. to 8 a.m. on weekdays and all day on weekends and holidays, said Hlicks.

He said the teletype is not continually watched during normal week-

day hours. Hlicks said a city administrative clerk handles dispatching duties from elsewhere in the Bamberg City Hall.

Darnell and Bamberg City Police Chief George Morris have proposed that the county and cities of Denmark and Bamberg centralize dispatching services for one year and fund an extra dispatcher.

Bamberg County already pays \$13,500 a year to the city for dispatching services while Denmark has its own police dispatchers.

County government officials agreed to consider a study of a central police dispatch during a meeting Thursday.

And Denmark Mayor Sam Neeley and County Councilman Isalah Odom agreed to ask their respective councils to consider funding an additional dispatcher for six months so that the



Sheriff Ed Darnell

county can regain access to the FBI computer.

Hlicks said if the proposal is approved, the county could have its access back before the end of the year.

to employ dispatcher

By BOB STUART
Greensboro Bureau

BAMBERG

Bamberg County has taken a step toward regaining access to the FBI national crime computer. It lost seven weeks ago.

Bamberg County Council and Denmark City Council voted Monday to appropriate \$4,000 each to fund the hiring of a temporary police dispatcher, who could be hired within a week, said Bamberg City Clerk Mack Clinkscales.

The dispatcher is needed to monitor the county teletype weekdays from 8 a.m. to 5 p.m.

The county's failure to provide around-the-clock, seven-day-a-week teletype monitoring by a dispatcher was cited Oct. 1 when the State Law Enforcement Division informed the county it could no longer enter data into the FBI computer.

Bamberg County was in violation of state and federal guidelines for computer use, said SLED Spokesman Hugh Munn.

Munn said Tuesday that Bamberg County could regain use of the FBI computer once it is in compliance.

The computer is used by law enforcement agencies to exchange information nationwide concerning stolen merchandise, weapons, criminals and missing persons.

Bamberg County Sheriff Ed Darnell said he and other law enforcement officials are reduced to telephoning out-of-state authorities to give information about crimes committed in the county.

Darnell said the county still can monitor FBI computer information.

Monday's action by the county and city councils also provides that County Council formulate a plan to centralize police dispatching in the county over the next six months, said Denmark Mayor Sam Neeley.

[469 US 221]

UNITED STATES, Petitioner

v

THOMAS J. HENSLEY

469 US 221, 83 L Ed 2d 604, 105 S Ct 675

[No. 83-1330]

Argued November 5, 1984. Decided January 8, 1985.

Decision: Investigative stop by police officers in reliance on "wanted flyer" issued by another police department held reasonable under Fourth Amendment.

SUMMARY

On certiorari, the United States Supreme Court reversed and remanded. In an opinion by O'CONNOR, J., expressing the unanimous view of the court, it was held (1) that if police have a reasonable suspicion, grounded in specific and articulable facts, that a person they encounter was involved in or is wanted in connection with a completed felony, they may make an investigatory stop in the absence of probable cause to arrest; (2) that police officers may make an investigative stop in objective reliance on a "wanted flyer" issued by another police department, so long as the flyer was issued on the basis of articulable facts supporting a reasonable suspicion that the wanted person has committed an offense; and (3) that the stop at issue was reasonable under the circumstances presented, and the evidence discovered during the stop was admissible.

BRENNAN, J., concurred, stating that the balancing test that replaces the probable cause standard in cases of investigative stops is appropriate as long as it is conducted with full regard for the serious privacy interests implicated even by such a relatively nonintrusive stop.

Several days after receiving a "wanted flyer" from a neighboring police department concerning a person suspected of involvement in an armed robbery, police officers made an investigative stop of the person named in the flyer. The stop was conducted while the suspect was in his automobile, accompanied by a passenger. Upon opening the passenger door, the officer observed the butt of a revolver protruding from underneath the passenger's

Briefs of Counsel, p 1104, *infra*.

UNITED STATES v HENSLEY

469 US 221, 83 L Ed 2d 604, 105 S Ct 675

seat. A search of the car conducted after the passenger's arrest uncovered two additional handguns. The robbery suspect was then arrested and subsequently indicted by a federal grand jury for being a convicted felon in possession of firearms. A motion to suppress the handguns from evidence was denied, the trial court concluding that the stop was proper, and the defendant was convicted as charged after a bench trial. The United States Court of Appeals for the Sixth Circuit reversed (713 F2d 220), concluding that investigative stops are restricted to settings involving the investigation of ongoing crimes, not completed ones such as the robbery at issue, that the flyer was insufficient to create a reasonable suspicion that the defendant had committed a crime, and that therefore his conviction rested on evidence obtained through an illegal arrest.

HEADNOTES

Classified to U.S. Supreme Court Digest, Lawyers' Edition

Arrest § 2 — investigatory stops — reliance on "wanted flyer"

1a-1c. If a "wanted flyer" or bulletin has been issued by a police department on the basis of articulable facts supporting a reasonable suspi-

cion that the wanted person has committed an offense, then objective reliance on that flyer by officers of another police department justifies a stop by such other officers to check identification, to pose questions to

TOTAL CLIENT-SERVICE LIBRARY* REFERENCES

- 68 Am Jur 2d, Searches and Seizures §§ 33, 58, 102.5, 103
- 8 Federal Procedure, L Ed, Criminal Procedure §§ 22:312, 22:313 12 Federal Procedure, L Ed, Evidence §§ 33:382 et seq.
- 5 Am Jur Trials 331, Excluding Illegally Obtained Evidence
- USCS, Constitution, 4th Amendment
- US L Ed Digest, Arrest § 2; Evidence § 681
- L Ed Index to Annos, Arrest; Search and Seizure
- ALR Quick Index, Arrest; Exclusion of Evidence; Search and Seizure
- Federal Quick Index, Stop and Frisk; Stop and Identify (Supp)
- Auto-Cite*: Any case citation herein can be checked for form, parallel references, later history and annotation references through the Auto-Cite computer research system.

ANNOTATION REFERENCES

Law enforcement officer's authority, under Federal Constitution, to "stop and frisk" person. 32 L Ed 2d 942.

What constitutes probable cause for arrest—Supreme Court cases. 28 L Ed 2d 978.

the person, or to detain the person briefly while attempting to obtain further information; if the flyer has been issued in the absence of a reasonable suspicion a stop in objective reliance upon it violates the Fourth Amendment, although in such a situation the officers making the stop may have a good-faith defense to any civil suit.

Arrest § 2 — investigatory stops — investigation of past criminal activity

2a-2c. The limits on the authority of police officers to stop a suspect to investigate past criminal activity are determined by balancing the nature and quality of the intrusion on personal security against the importance of the governmental interests alleged to justify the intrusion; when this balancing test is applied to stops to investigate past crimes, probable cause to arrest need not always be required; thus, if police have a reasonable suspicion, grounded in specific and articulable facts, that a person they encounter was involved in or is wanted in connection with a completed felony, they may make an investigatory stop in the absence of probable cause.

Evidence § 681 — admissibility — evidence uncovered during investigatory stop — reliance on "wanted flyer"

3. Evidence uncovered by police in the course of an investigatory stop in objective reliance on another police department's "wanted flyer" or bulletin is admissible in evidence in a subsequent criminal prosecution if

the police who issued the flyer possessed a reasonable suspicion justifying a stop and if the stop that in fact occurred was not significantly more intrusive than a stop that the issuing department would have been permitted to make.

Arrest § 2 — investigatory stops — investigation of past criminal activity

4. Police officers who possess a reasonable suspicion that a person was involved in an armed robbery, based on detailed and sufficiently reliable information provided by an informer, are justified in making an investigatory stop of the suspect after the robbery is completed; a brief stop and detention at the earliest opportunity after the suspicion arises is fully consistent with Fourth Amendment principles.

Arrest § 2 — investigatory stops — reliance on "wanted flyer"

5a, 5b. An investigatory stop of a suspected robber by police officers in reliance on a "wanted flyer" issued by a neighboring police department is reasonable under the Fourth Amendment, and handguns uncovered in the course of the stop are admissible in evidence in a subsequent criminal prosecution, where the detention is brief, where a reasonable suspicion underlies and supports issuance of the flyer, and where the stop is reasonable in objective reliance on the flyer and is not significantly more intrusive than a stop that the issuing department would have been permitted to make.

SYLLABUS BY REPORTER OF DECISIONS

Following an armed robbery in the Cincinnati suburb of St. Bernard, Ohio, a St. Bernard police officer, on

the basis of information obtained from an informant that respondent had driven the getaway car during

the robbery, issued a "wanted flyer" to other police departments in the area. The flyer stated that respondent was wanted for investigation of the robbery, described him and the date and location of the robbery, and asked the other departments to pick up and hold him for the St. Bernard police. Subsequently, on the basis of the flyer and after inquiring without success as to whether a warrant was outstanding for respondent's arrest, police officers from Covington, Ky., another Cincinnati suburb, stopped an automobile that respondent was seen driving. One of the officers recognized a passenger in the car as a convicted felon and, upon observing a revolver butt protruding from underneath the passenger's seat, arrested the passenger. After a search of the car uncovered other handguns, respondent was also arrested. Respondent was then indicted on the federal charge of being a convicted felon in possession of firearms. Respondent moved to suppress the handguns from evidence on the grounds that the Covington police had stopped him in violation of the Fourth Amendment and the principles announced in *Terry v Ohio*, 392 US 1, 20 L Ed 2d 889, 88 S Ct 1868, 44 Ohio Ops 2d 383. The Federal District Court denied respondent's motion, and he was convicted. The Court of Appeals reversed, holding that the stop of respondent's car was improper because the crime being investigated was not imminent or ongoing, but rather was already completed, that the "wanted flyer" was insufficient to create a reasonable suspicion that respondent had committed a crime, and that therefore his conviction rested on evidence obtained through an illegal arrest.

Held:

1. Where police have been unable to locate a person suspected of involvement in a past crime, the ability to briefly stop that person, ask questions, or check identification in the absence of probable cause promotes the strong government interest in solving crimes and bringing offenders to justice. Restraining police action until after probable cause is obtained would not only hinder the investigation but might also enable the suspect to flee and remain at large. The law enforcement interests at stake in these circumstances outweigh the individual's interest to be free of a stop and detention that is no more extensive than permissible in the investigation of imminent or ongoing crimes. When police have a reasonable suspicion, grounded in specific and articulable facts, that a person they encounter was involved in or is wanted in connection with a completed felony, then a *Terry* stop may be made to investigate that suspicion.

2. If a "wanted flyer" has been issued on the basis of articulable facts supporting a reasonable suspicion that the person wanted has committed an offense, then reliance on that flyer justifies a stop to check identification, to pose questions, or to detain the person briefly while attempting to obtain further information. It is the objective reading of the flyer that determines whether police officers from a department other than the one that issued the flyer can defensibly act in reliance on it. Assuming that the police make a *Terry* stop in objective reliance on a flyer, the evidence uncovered in the course of the stop is admissible if the police who issued the flyer possessed a reasonable suspicion justify-

ing the stop, and if the stop that occurred was not significantly more intrusive than would have been permitted the issuing department.

3. Under the above principles, the investigatory stop of respondent was reasonable under the Fourth Amendment, and therefore the evidence discovered during the stop was admissible. The justification for a stop did not evaporate when the armed robbery was completed. Respondent was reasonably suspected of involvement in a felony and was at large from the time the suspicion arose until the stop by the Covington police. A brief stop and detention at the earliest opportunity after

the suspicion arose was fully consistent with Fourth Amendment principles. The flyer issued by the St. Bernard police, objectively read and supported by a reasonable suspicion on the part of the issuing department, justified the length and intrusiveness of the stop and detention that occurred. And it is irrelevant whether the Covington police intended to detain respondent only long enough to confirm the existence of a warrant, or for a longer period.

713 F2d 220, reversed and remanded.

O'Connor, J., delivered the opinion for a unanimous Court. Brennan, J., filed a concurring opinion.

APPEARANCES OF COUNSEL

Kathryn A. Oberly argued the cause for petitioner.

Edward G. Drennen, II argued the cause for respondent.

Briefs of Counsel, p 1104, *infra*.

OPINION OF THE COURT

[469 US 223]

[1a] Justice O'Connor delivered the opinion of the Court.

We granted certiorari in this case, 467 US 1203, 81 L Ed 2d 342, 104 S Ct 2383 (1984), to determine whether police officers may stop and briefly detain a person who is the subject of a "wanted flyer" while they attempt to find out whether an arrest warrant has been issued. We conclude that such stops are consistent with the Fourth Amendment under appropriate circumstances.

I

On December 4, 1981, two armed men robbed a tavern in the Cincinnati suburb of St. Bernard, Ohio. Six days later, a St. Bernard police officer, Kenneth Davis, interviewed an informant who passed along information that respondent Thomas Hensley had driven the getaway car

during the armed robbery. Officer Davis obtained a written statement from the informant and immediately issued a "wanted flyer" to other police departments in the Cincinnati metropolitan area.

The flyer twice stated that Hensley was wanted for investigation of an aggravated robbery. It described both Hensley and the date and location of the alleged robbery, and asked other departments to pick up and hold Hensley for the St. Bernard police in the event he were located. The flyer also warned other departments to use caution and to consider Hensley armed and dangerous.

The St. Bernard Police Department's "wanted flyer" was received by teletype in the headquarters of the Covington Police Department on December 10, 1981. Covington is a

Kentucky suburb of Cincinnati that is approximately five miles from St. Bernard. The flyer was read aloud at each change of shift in the Covington Police Department between December 10 and December 16, 1981. Some of the Covington officers were acquainted with Hensley, and after December 10 they periodically looked for him at places in Covington he was known to frequent.

On December 16, 1981, Covington Officer Terence Eger saw a white Cadillac convertible stopped in the middle of a

[469 US 224]

Covington street. Officer Eger saw Hensley in the driver's seat and asked him to move on. As Hensley drove away, Eger inquired by radio whether there was a warrant outstanding for Hensley's arrest. Before the dispatcher could answer, two other Covington officers who were in separate cars on patrol interrupted to say that there might be an Ohio robbery warrant outstanding on Hensley. The officers, Daniel Cope and David Rassache, subsequently testified that they had heard or read the St. Bernard flyer on several occasions, that they recalled that the flyer sought a stop for investigation only, and that in their experience the issuance of such a flyer was usually followed by the issuance of an arrest warrant. While the dispatcher checked to see whether a warrant had been issued, Officer Cope drove to a Holman Street address where Hensley occasionally stayed, and Officer Rassache went to check a second location.

The dispatcher had difficulty in confirming whether a warrant had been issued. Unable to locate the flyer, she called the Cincinnati Police Department on the mistaken belief that the flyer had originated

in Cincinnati. The Cincinnati Police Department transferred the call to its records department, which placed the dispatcher on hold. In the meantime, Officer Cope reported that he had sighted a white Cadillac approaching him on Holman Street. Cope turned on his flashing lights and Hensley pulled over to the curb. Before Cope left his patrol car, the dispatcher advised him that she had "Cincinnati hunting for the warrant," App 49, but that she had not yet confirmed it. Cope approached Hensley's car with his service revolver drawn and pointed into the air. He had Hensley and a passenger seated next to him step out of the car.

Moments later, Officer Rassache arrived in his separate car. He recognized the passenger, Albert Green, a convicted felon. Rassache stepped up to the open passenger door of Hensley's car and observed the butt of a revolver protruding from underneath the passenger's seat. Green

[469 US 225]

was then arrested. A search of the car uncovered a second handgun wrapped in a jacket in the middle of the front seat and a third handgun in a bag in the back seat. After the discovery of these weapons, Hensley was also arrested.

After state handgun possession charges against Hensley were dismissed, Hensley was indicted by a federal grand jury in the Eastern District of Kentucky for being a convicted felon in possession of firearms in violation of 18 USC App § 1202(a)(1) [18 USCS Appx § 1202(a)(1)]. Hensley moved to suppress the handguns from evidence on the grounds that the Covington police had impermissibly stopped him in violation of the Fourth Amendment and the principles an-

nounced in *Terry v Ohio*, 392 US 1, 20 L Ed 2d 889, 88 S Ct 1868, 44 Ohio Ops 2d 383 (1968). The District Judge held the stop to be proper and denied the motion. Respondent was convicted after a bench trial and sentenced to two years in federal prison.

The United States Court of Appeals for the Sixth Circuit reversed the conviction. 713 F2d 220 (1983). The panel noted that the Covington police could not justifiably conclude from the St. Bernard flyer that a warrant had been issued for Hensley's arrest; nor could the Covington police stop the respondent while they attempted to find out whether a warrant had in fact been issued. Reviewing this Court's decisions applying *Terry*, the Sixth Circuit concluded that investigative stops remain a narrow exception to the probable-cause requirement, and that this Court has manifested a "clear intention to restrict investigative stops to settings involving the investigation of ongoing crimes." 713 F2d, at 225. Since Covington police encountered Hensley almost two weeks after the armed robbery in St. Bernard, they had no reason to believe they were investigating an ongoing crime. Because the Covington police were familiar only with the St. Bernard flyer, and not with the specific information which led the St. Bernard police to issue the flyer, the Court of Appeals held they lacked a reasonable suspicion sufficient to justify an investigative stop. The Court of Appeals concluded that Hensley's conviction rested on evidence obtained

(489 US 226)

through an illegal arrest, and therefore had to be reversed. We disagree, and now reverse.

II

The Fourth Amendment protects

the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. In *Terry*, *supra*, and subsequent cases, this Court has held that, consistent with the Fourth Amendment, police may stop persons in the absence of probable cause under limited circumstances. See *Dunaway v New York*, 442 US 200, 207-211, 60 L Ed 2d 824, 99 S Ct 2248 (1979). In particular, the Court has noted that law enforcement agents may briefly stop a moving automobile to investigate a reasonable suspicion that its occupants are involved in criminal activity. See *United States v Brignoni-Ponce*, 422 US 873, 881, 45 L Ed 2d 607, 95 S Ct 2574 (1975) (within United States borders, Government interest in preventing illegal entry of aliens permits a *Terry* stop on reasonable suspicion that particular vehicle contains aliens). Although stopping a car and detaining its occupants constitute a seizure within the meaning of the Fourth Amendment, the governmental interest in investigating an officer's reasonable suspicion, based on specific and articulable facts, may outweigh the Fourth Amendment interest of the driver and passengers in remaining secure from the intrusion. See *Delaware v Prouse*, 440 US 648, 653-655, 59 L Ed 2d 660, 99 S Ct 1391 (1979).

In this case, the Sixth Circuit announced two prerequisites to such an investigatory stop and held that they were lacking: first, the crime being investigated was not imminent or ongoing, but rather was already completed; second, the "wanted flyer" was insufficient to create a reasonable suspicion that respondent had engaged in criminal activity. If either part of this analysis is correct,

UNITED STATES v HENSLEY

469 US 221, 83 L Ed 2d 604, 105 S Ct 675

en it was indeed improper to stop respondent, and his conviction cannot stand. We accordingly turn to the separate but related issues of Terry stops to investigate completed crimes and Terry stops in reliance on another police department's "wanted flyer."

[469 US 227]

A

This is the first case we have addressed in which police stopped a person because they suspected he was involved in a completed crime. In our previous decisions involving investigatory stops on less than probable cause, police stopped or seized a person because they suspected he was about to commit a crime, e.g., Terry, supra, or was committing a crime at the moment of the stop, e.g., Adams v Williams, 407 US 143, 32 L Ed 2d 612, 92 S Ct 1921 (1972). Noting that Florida v Royer, 460 US 491, 75 L Ed 2d 229, 103 S Ct 1319 (1983), struck down a particularly intrusive detention of a person suspected of committing an ongoing crime, the Court of Appeals in this case concluded that we clearly intended to restrict investigative stops to the context of ongoing crimes.

[2a] We do not agree with the Court of Appeals that our prior opinions contemplate an inflexible rule that precludes police from stopping persons they suspect of past criminal activity unless they have probable cause for arrest. To the extent previous opinions have addressed the issue at all, they have suggested that some investigative stops based on a reasonable suspicion of past criminal activity could withstand Fourth Amendment scrutiny. Thus United States v Cortez, 449 US 411, 417, n

2, 66 L Ed 2d 621, 101 S Ct 690 (1981), indicates in a footnote that "[o]f course, an officer may stop and question a person if there are reasonable grounds to believe that person is wanted for past criminal conduct." And in United States v Place, 462 US 696, 77 L Ed 2d 110, 103 S Ct 2637 (1983), decided barely a month before the Sixth Circuit's opinion, this Court stated that its prior opinions acknowledged police authority to stop a person "when the officer has reasonable, articulable suspicion that the person *has been*, is, or is about to be engaged in criminal activity." Id., at 702. 77 L Ed 2d 110, 103 S Ct 2637 (emphasis added). See also Michigan v Summers, 452 US 692, 699, and n 7, 69 L Ed 2d 340, 101 S Ct 2587 (1981). Indeed, Florida v Royer itself suggests that certain seizures are justifiable under the Fourth Amendment even in the absence of probable cause "if there is articulable suspicion that a person *has committed* or is about to commit a crime." 460 US, at 498, 75 L Ed 2d 229, 103 S Ct 1319 (plurality opinion) (emphasis added).

[469 US 228]

[2b] At the least, these dicta suggest that the police are not automatically shorn of authority to stop a suspect in the absence of probable cause merely because the criminal has completed his crime and escaped from the scene. The precise limits on investigatory stops to investigate past criminal activity are more difficult to define. The proper way to identify the limits is to apply the same test already used to identify the proper bounds of intrusions that further investigations of imminent or ongoing crimes. That test, which is grounded in the standard of reasonableness embodied in the Fourth Amendment, balances the nature

and quality of the intrusion on personal security against the importance of the governmental interests alleged to justify the intrusion. *United States v Place*, supra, at 703, 77 L Ed 2d 110, 103 S Ct 2637; *Michigan v Summers*, supra, at 698-701, 69 L Ed 2d 340, 101 S Ct 2587. When this balancing test is applied to stops to investigate past crimes, we think that probable cause to arrest need not always be required.

The factors in the balance may be somewhat different when a stop to investigate past criminal activity is involved rather than a stop to investigate ongoing criminal conduct. This is because the governmental interests and the nature of the intrusions involved in the two situations may differ. As we noted in *Terry*, one general interest present in the context of ongoing or imminent criminal activity is "that of effective crime prevention and detection." *Terry*, 392 US, at 22, 20 L Ed 2d 889, 88 S Ct 1868, 44 Ohio Ops 2d 383. A stop to investigate an already completed crime does not necessarily promote the interest of crime prevention as directly as a stop to investigate suspected ongoing criminal activity. Similarly, the exigent circumstances which require a police officer to step in before a crime is committed or completed are not necessarily as pressing long afterwards. Public safety may be less threatened by a suspect in a past crime who now appears to be going about his lawful business than it is by a suspect who is currently in the process of violating the law. Finally, officers making a stop to investigate past crimes may have a wider range of opportunity to

Texas, 443 US 47, 51, 61 L Ed 2d 357, 99 S Ct 2637 (1979); ALI Model Code of Pre-Arrest Procedure 12 (Prop. Off. Draft No. 1, 1972).

Despite these differences, where police have been unable to locate a person suspected of involvement in a past crime, the ability to briefly stop that person, ask questions, or check identification in the absence of probable cause promotes the strong government interest in solving crimes and bringing offenders to justice. Restraining police action until after probable cause is obtained would not only hinder the investigation, but might also enable the suspect to flee in the interim and to remain at large. Particularly in the context of felonies or crimes involving a threat to public safety, it is in the public interest that the crime be solved and the suspect detained as promptly as possible. The law enforcement interests at stake in these circumstances outweigh the individual's interest to be free of a stop and detention that is no more extensive than permissible in the investigation of imminent or ongoing crimes.

[2c] We need not and do not decide today whether *Terry* stops to investigate all past crimes, however serious, are permitted. It is enough to say that, if police have a reasonable suspicion, grounded in specific and articulable facts, that a person they encounter was involved in or is wanted in connection with a completed felony, then a *Terry* stop may be made to investigate that suspicion. The automatic barrier to such stops erected by the Court of Appeals accordingly cannot stand.

B

[469 US 229]
choose the time and circumstances of the stop. See *Brown v*
612

[1b] At issue in this case is a stop of a person by officers of one police

UNITED STATES v HENSLEY
469 US 221, 83 L Ed 2d 604, 105 S Ct 675

partment in reliance on a flyer issued by another department indicating that the person is wanted for investigation of a felony. The Court of Appeals concluded that "the Fourth Amendment does not permit police officers in one department to seize a person simply because a neighboring

[469 US 230]

police department has circulated a flyer reflecting the desire to question that individual about some criminal investigation that does not involve the arresting officers or their department." 713 F2d, at 225. This holding apparently rests on the omission from the flyer of the specific and articulable facts which led the first department to suspect respondent's involvement in a completed crime. *Ibid*.

This Court discussed a related issue in *Whiteley v Warden*, 401 US 560, 28 L Ed 2d 306, 91 S Ct 1031, 58 Ohio Ops 2d 434 (1971). In *Whiteley*, a county sheriff in Wyoming obtained an arrest warrant for a person suspected of burglary. The sheriff then issued a message through a statewide law enforcement radio network describing the suspect, his car, and the property taken. At least one version of the message also indicated that a warrant had been issued. *Id.*, at 564, and n 5, 28 L Ed 2d 306, 91 S Ct 1031, 58 Ohio Ops 2d 434. The message did not specify the evidence that gave the sheriff probable cause to believe the suspect had committed the breaking and entering. In reliance on the radio message, police in Laramie stopped the suspect and searched his car. The Supreme Court, in an opinion by Justice Harlan, ultimately concluded that the sheriff had lacked probable cause to obtain the warrant and that the evidence obtained during the search

by the police in Laramie had to be excluded. In so ruling, however, the Court noted:

"We do not, of course, question that the Laramie police were entitled to act on the strength of the radio bulletin. Certainly police officers called upon to aid other officers in executing arrest warrants are entitled to assume that the officers requesting aid offered the magistrate the information requisite to support an independent judicial assessment of probable cause. Where, however, the contrary turns out to be true, an otherwise illegal arrest cannot be insulated from challenge by the decision of the investigating officer to rely on fellow officers to make the arrest." *Id.*, at 568, 28 L Ed 2d 306, 91 S Ct 1031, 58 Ohio Ops 2d 434.

This language in *Whiteley* suggests that, had the sheriff who issued the radio bulletin possessed probable cause for

[469 US 231]

arrest, then the Laramie police could have properly arrested the defendant even though they were unaware of the specific facts that established probable cause. See *United States v Maryland*, 479 F2d 566, 569 (CA5 1973). Thus *Whiteley* supports the proposition that, when evidence is uncovered during a search incident to an arrest in reliance merely on a flyer or bulletin, its admissibility turns on whether the officers who issued the flyer possessed probable cause to make the arrest. It does not turn on whether those relying on the flyer were themselves aware of the specific facts which led their colleagues to seek their assistance. In an era when criminal suspects are increasingly mobile and increasingly likely to flee across jurisdictional boundaries, this

rule is a matter of common sense: it minimizes the volume of information concerning suspects that must be transmitted to other jurisdictions and enables police in one jurisdiction to act promptly in reliance on information from another jurisdiction.

Neither respondent nor the Court of Appeals suggests any reason why a police department should be able to act on the basis of a flyer indicating that another department has a warrant, but should not be able to act on the basis of a flyer indicating that another department has a reasonable suspicion of involvement with a crime. Faced with this precise issue, the Court of Appeals for the Ninth Circuit applied *Whiteley* and concluded that, although the officer who issues a wanted bulletin must have a reasonable suspicion sufficient to justify a stop, the officer who acts in reliance on the bulletin is not required to have personal knowledge of the evidence creating a reasonable suspicion. *United States v Robinson*, 536 F2d 1298, 1300 (1976). The Ninth Circuit there noted "that effective law enforcement cannot be conducted unless police officers can act on directions and information transmitted by one officer to another and that officers, who must often act swiftly, cannot be expected to cross-examine their fellow officers about the foundation for the transmitted information." *Id.*, at 1299.

[469 US 232]

It could be argued that police can more justifiably rely on a report that a magistrate has issued a warrant than on a report that another law enforcement agency has simply concluded that it has a reasonable suspicion sufficient to authorize an investigatory stop. We do not find this

distinction significant. The law enforcement interests promoted by allowing one department to make investigatory stops based upon another department's bulletins or flyers are considerable, while the intrusion on personal security is minimal. The same interests that weigh in favor of permitting police to make a Terry stop to investigate a past crime, *supra*, at 229, 83 L Ed 2d, at 612, support permitting police in other jurisdictions to rely on flyers or bulletins in making stops to investigate past crimes.

[1c, 3] We conclude that, if a flyer or bulletin has been issued on the basis of articulable facts supporting a reasonable suspicion that the wanted person has committed an offense, then reliance on that flyer or bulletin justifies a stop to check identification, see *United States ex rel. Kirby v Sturges*, 510 F2d 397, 400-401 (CA7) (Stevens, J.), cert denied, 421 US 1016, 44 L Ed 2d 685, 95 S Ct 2424 (1975), to pose questions to the person, or to detain the person briefly while attempting to obtain further information. See *Adams v Williams*, 407 US 143, 146, 32 L Ed 2d 612, 92 S Ct 1921 (1972) ("A brief stop of a suspicious individual, in order to determine his identity or to maintain the status quo momentarily while obtaining more information, may be the most reasonable in light of the facts known to the officer at the time"). If the flyer has been issued in the absence of a reasonable suspicion, then a stop in the objective reliance upon it violates the Fourth Amendment. In such a situation, of course, the officers making the stop may have a good-faith defense to any civil suit. See *Scheuer v Rhodes*, 416 US 232, 40 L Ed 2d 90, 94 S Ct 1683, 71 Ohio Ops 2d 474 (1974); *Pierson v Ray*, 386 US 547,

UNITED STATES v HENSLEY

469 US 221, 83 L Ed 2d 604, 105 S Ct 675

18 L Ed 2d 288, 87 S Ct 1213 (1967); *Turner v Raynes*, 611 F2d 92, 93 (CA5) (officer relying in good faith on an invalid arrest warrant has defense to civil suit), cert denied, 449 US 900, 66 L Ed 2d 129, 101 S Ct 269 (1980). It is the objective reading of the flyer or bulletin that determines whether other

[469 US 233]

police officers can defensibly act in reliance on it. Cf. *Terry*, 392 US, at 21-22, 20 L Ed 2d 889, 88 S Ct 1868, 44 Ohio Ops 2d 383 ("it is imperative that the facts be judged against an objective standard: would the facts available to the officer at the moment of the seizure or the search 'warrant a man of reasonable caution in the belief that the action taken was appropriate?'). Assuming the police make a *Terry* stop in objective reliance on a flyer or bulletin, we hold that the evidence uncovered in the course of the stop is admissible if the police who issued the flyer or bulletin possessed a reasonable suspicion justifying a stop, *United States v Robinson*, supra, and if the stop that in fact occurred was not significantly more intrusive than would have been permitted the issuing department.

III

It remains to apply the two sets of principles described above to the stop and subsequent arrest of respondent Hensley.

At the outset, we assume, arguendo, that the St. Bernard police who issued the "wanted flyer" on Hensley lacked probable cause for his arrest. The District Court implied that the St. Bernard police had probable cause for arrest, but held only that the St. Bernard officers had reasonable suspicion sufficient

to justify a stop. App to Pet for Cert 14a. The Court of Appeals implied that probable cause might be lacking, 713 F2d, at 223, but ultimately concluded that the question was irrelevant because the Covington police would not be entitled to make an arrest or a stop regardless of whether the St. Bernard police possessed probable cause or a reasonable suspicion. In this Court, no party contends that the St. Bernard police had probable cause to arrest Hensley.

[4] We agree with the District Court that the St. Bernard police possessed a reasonable suspicion, based on specific and articulable facts, that Hensley was involved in an armed robbery. The District Judge heard testimony from the St. Bernard officer who interviewed the informant. On the strength of the evidence, the District Court concluded

[469 US 234]

that the wealth of detail concerning the robbery revealed by the informant, coupled with her admission of tangential participation in the robbery, established that the informant was sufficiently reliable and credible "to arouse a reasonable suspicion of criminal activity by [Hensley] and to constitute the specific and articulable facts needed to underlie a stop." App to Pet for Cert 14a. Under the circumstances, "the information carried enough indicia of reliability," *Adams v Williams*, supra, at 147, 32 L Ed 2d 612, 92 S Ct 1921, to justify an investigatory stop of Hensley.

The justification for a stop did not evaporate when the armed robbery was completed. Hensley was reasonably suspected of involvement in a felony and was at large from the time the suspicion arose until the stop by the Covington police. A brief

615

stop and detention at the earliest opportunity after the suspicion arose is fully consistent with the principles of the Fourth Amendment.

[5a] Turning to the flyer issued by the St. Bernard police, we believe it satisfies the objective test announced today. An objective reading of the entire flyer would lead an experienced officer to conclude that Thomas Hensley was at least wanted for questioning and investigation in St. Bernard. Since the flyer was issued on the basis of articulable facts supporting a reasonable suspicion, this objective reading would justify a brief stop to check Hensley's identification, pose questions, and inform the suspect that the St. Bernard police wished to question him. As an experienced officer could well assume that a warrant might have been obtained in the period after the flyer was issued, we think the flyer would further justify a brief detention at the scene of the stop while officers checked whether a warrant had in fact been issued. It is irrelevant whether the Covington officers intended to detain Hensley only long enough to confirm the existence of a warrant, or for some longer period; what matters is that the stop and detention that occurred were

[469 US 235]

in fact no more intrusive than would have been permitted an experienced officer on an objective reading of the flyer.

To be sure, the St. Bernard flyer at issue did not request that other police departments briefly detain Hensley merely to check his identification or confirm the existence of a warrant. Instead, it asked other departments to pick up and hold Hensley for St. Bernard. Our decision today does not suggest that such a

detention, whether at the scene or at the Covington police headquarters, would have been justified. Given the distance involved and the time required to identify and communicate with the department that issued the flyer, such a detention might well be so lengthy or intrusive as to exceed the permissible limits of a Terry stop. See *United States v Place*, 462 US, at 709, 77 L Ed 2d 110, 103 S Ct 2637. Nor do we mean to endorse St. Bernard's request in its flyer for actions that could foreseeably violate the Fourth Amendment. We hold only that this flyer, objectively read and supported by a reasonable suspicion on the part of the issuing department, justified the length and intrusiveness of the stop and detention that actually occurred.

When the Covington officers stopped Hensley, they were authorized to take such steps as were reasonably necessary to protect their personal safety and to maintain the status quo during the course of the stop. The Covington officers' conduct was well within the permissible range in the context of suspects who are reported to be armed and dangerous. See *Michigan v Long*, 463 US 1032, 1049-1050, 77 L Ed 2d 1201, 103 S Ct 3469 (1983); *Pennsylvania v Mimms*, 434 US 106, 110-111, 54 L Ed 2d 331, 98 S Ct 330 (1977) (per curiam). Having stopped Hensley, the Covington police were entitled to seize evidence revealed in plain view in the course of the lawful stop, to arrest Hensley's passenger when evidence discovered in plain view gave probable cause to believe the passenger had committed a crime, *Texas v Brown*, 460 US 730, 75 L Ed 2d 502, 103 S Ct 1535 (1983) (plurality opinion), and subsequently to search the passenger compartment of the car because it was

within the passenger's immediate control. New York
[469 US 236]

v Belton, 453 US
454, 69 L Ed 2d 768, 101 S Ct 2860
(1981). Finally, having discovered additional weapons in Hensley's car during the course of a lawful search, the Covington officers had probable cause to arrest Hensley himself for possession of firearms.

[5b] The length of Hensley's detention from his stop to his arrest on probable cause was brief. A reasonable suspicion on the part of the St. Bernard police underlies and sup-

ports their issuance of the flyer. Finally, the stop that occurred was reasonable in objective reliance on the flyer and was not significantly more intrusive than would have been permitted the St. Bernard police. Under these circumstances, the investigatory stop was reasonable under the Fourth Amendment, and the evidence discovered during the stop was admissible.

The judgment of the Court of Appeals is reversed, and the case is remanded for proceedings consistent with this opinion.

It is so ordered.

SEPARATE OPINION

Justice Brennan, concurring.

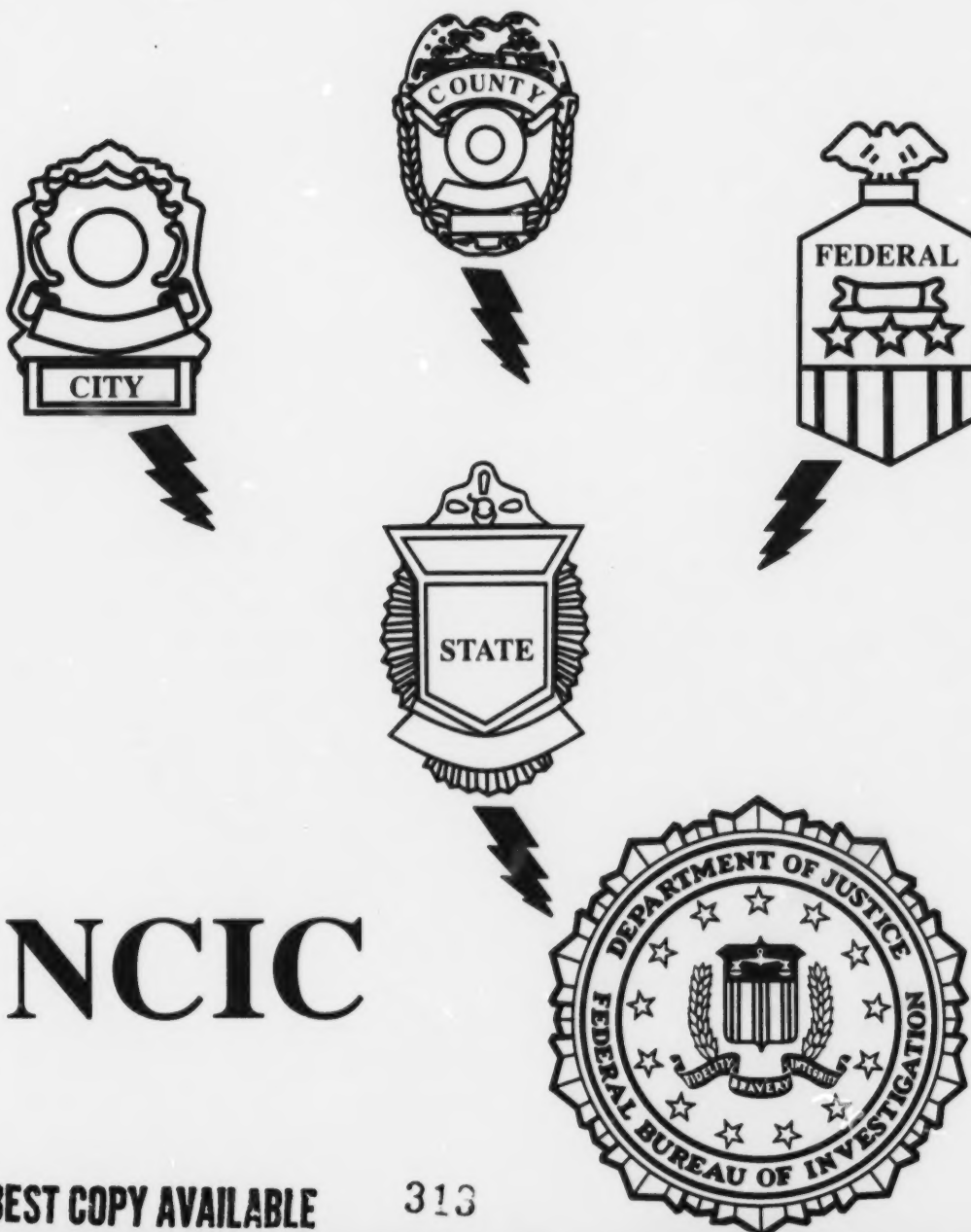
I join the opinion of the Court. With respect to its effect on respondent's "right . . . to be secure . . . in [his] perso[n]" guaranteed by the Fourth Amendment, the stop in this case—although it no doubt seriously fringed upon respondent's privacy—lasted a mere matter of moments, see ante, at 224-225, 83 L Ed 2d, at 609, before the discovery of the gun ripened what had been merely reasonable suspicion into the full-scale probable cause necessary for an arrest. For circumstances like these, *Terry v Ohio*, 392 US 1, 20 L Ed 2d 889, 88 S Ct 1868, 44 Ohio Ops 2d 383 (1968), "defined a special category of Fourth Amendment 'seizures' so substantially less intrusive than arrests that the general rule

requiring probable cause to make Fourth Amendment 'seizures' reasonable could be replaced by a balancing test." *Dunaway v New York*, 442 US 200, 210, 60 L Ed 2d 824, 99 S Ct 2248 (1979). See ante, at 228, 83 L Ed 2d, at 611-612. Such a balancing test is appropriate as long as it is conducted with full

[469 US 237]

regard for the serious privacy interests implicated even by such a relatively nonintrusive stop. See *Terry v Ohio*, supra. Of course, in the case of intrusions properly classifiable as full-scale arrests for Fourth Amendment purposes, no such balancing test is needed. Such arrests are governed by the probable-cause standard provided by the text of the Fourth Amendment itself.

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: VALIDATION

TITLE OF INSTRUCTION:

VALIDATION

TIME ALLOTTED:

30 MINUTES

TARGET GROUP:

FULL ACCESS TERMINAL OPERATORS

INSTRUCTOR:

METHOD OF INSTRUCTION:

LECTURE, OVERHEAD
TRANSPARENCIES, AND VIDEOTAPE

DATE:

7/1/92

NCIC VALIDATION LESSON PLAN TABLE OF CONTENTS

STATEMENT OF GOAL AND OBJECTIVE	VAL-1
CRITERION TEST	VAL-2
CRITERION TEST ANSWERS	VAL-3
ITEMS AND MATERIALS	VAL-5
INTRODUCTION	VAL-6
DEFINITION OF VALIDATION	VAL-6
THE VALIDATION PROCESS	VAL-8
NCIC	VAL-9
The CTO or SC	VAL-9
The Validating Agency	VAL-9
VALIDATION CERTIFICATION	VAL-12
VALIDATION DOCUMENTATION	VAL-13
CONCLUSION	VAL-13
BIBLIOGRAPHY	VAL-15

STATEMENT OF GOAL AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator critical information on the policies and procedures for the NCIC validation process.

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the operator will be able to:

1. State the validation policy.
2. State how often NCIC records are validated.
3. State the NCIC Files that must be validated.
4. State the responsibilities of the Control Terminal Agency (CTA) or Service Coordinator (SC) in the validation process.
5. List the validation procedures that must be followed by the validating agency.
6. List the methods by which recent consultation can be made for wanted persons, vehicles, and missing person records.
7. Explain the significance of validation certification.

CRITERION TEST

1. State the validation policy.
2. Validation is required for all NCIC "Hot" Files except _____.
3. An NCIC record is initially validated within 120 days of entry.
 - A. True.
 - B. False.
4. State the responsibilities of the Control Terminal Officer (CTO) in the validation process.
5. Explain the process the validating agency must follow to properly validate an NCIC record.
6. Name three methods by which an agency can make recent consultation for vehicle records.
7. A lack of validation procedures or documentation by the validating agency will not effect the results of an NCIC Audit.
 - A. True.
 - B. False.
8. Describe the action that may be taken if records are not properly validated or if the certification letter is not returned.

CRITERION TEST ANSWERS

1. Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during an NCIC Audit.
2. Validation is required for all NCIC "Hot" Files except the Article File.
3. False. An NCIC record is initially validated within 90 days of entry into the NCIC System.
4. The CTO or SC is responsible for disseminating the validation listings to the appropriate agency for certification.

The CTO or SC is also responsible for ensuring that the validating agencies certify their records and return the certification documents within the allotted time.

5. a. The validating agency, upon receipt of the validation listing from the CTO or SC, must compare every record on the listing against supporting documentation such as case files, incident reports, and warrants to ensure accuracy, validity, and completeness of the data entered in the NCIC record.
- b. A second step is necessary for validation of wanted person, vehicle, and missing person records. To ensure validity of the NCIC record, the validating agency is required to make a recent consultation with the prosecutor or court with respect to the wanted person records and with the complainant, victim, motor registry files, or other appropriate source or individual with regards to vehicle and missing person records.

6. Recent consultation with the appropriate individual for vehicle records can be accomplished by:
 - a. telephone call
 - b. personal visit
 - c. letter or postcard.
7. False. Failure to have either procedures or documentation will result in a higher risk assessment of the agency by the NCIC Audit Staff.
8. If an agency fails to properly validate its records or return the certification letter, the state will purge that agency's unvalidated records.

If a CTO or SC fails to return the certification letter, the CTO or SC will be subject to sanctions from the Advisory Policy Board.

ITEMS AND MATERIALS

Overhead Projector and Screen

Overhead Transparencies:

- VAL-OH #1 - Title of Program
- VAL-OH #2 - Definition of Validation
- VAL-OH #3 - Validation Procedures
- VAL-OH #4 - Validation Certification
- VAL-OH #5 - Course Summary

Handout Materials:

- VAL-HD #1 - NCIC Validation Schedule
- VAL-HD #2 - NCIC Acknowledgement Letter
- VAL-HD #3 - NCIC Certification Letter
- VAL-HD #4 - NCIC Audit Staff Recent Consultation Letter for NCIC
Vehicle Records
- VAL-HD #5 - Newspaper Clippings

VCR and Monitor

Videotape:

NCIC Validation

7/1/92

VAL-5

I. INTRODUCTION

REFERENCES

THIS 30-MINUTE BLOCK OF INSTRUCTION IS DESIGNED TO IDENTIFY NCIC POLICY AND PROCEDURES INVOLVED IN COMPLETING VALIDATIONS.

OH #1

In July, 1987, the city of Los Angeles was found liable and ordered to pay \$55,000 in damages for failure to follow established NCIC policy requirements. The case, which began with the failure of a police department to maintain complete and accurate records, represents a warning that the courts will not tolerate negligent use of NCIC.

NCIC has established a specific policy known as validation. This policy requires entering agencies to verify NCIC records once a year.

II. DEFINITION OF VALIDATION

OH #2

Validation is the process through which the validating agency confirms, on an annual basis, that each NCIC record is complete, accurate, and still outstanding or active.

The NCIC Technical and Operational Update (TOU) 89-5 published the current NCIC Validation Policy.

IO #1

The policy reads as follows:

"Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is

7/1/92

VAL-6

517.

accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during an NCIC Audit."

INSTRUCTOR'S NOTE: EFFECTIVE PER THE NCIC TOU 89-5, THE VALIDATION POLICY NO LONGER REQUIRES RECENT CONSULTATION WITH THE COMPLAINANT ON BOAT FILE RECORDS.

An NCIC record is initially validated within 90 days of entry into the NCIC System. The record must then be validated each year it remains in the system.

Validation is required for all NCIC "Hot" Files except the Article File. The following NCIC Files are validated by the respective agencies:

1. U.S. Secret Service Protective File - validated by the U.S. Secret Service, the entering agency for U.S. Secret Service protective records (Refer to the U.S. Secret Service Protective File Lesson Plan for more information).
2. Foreign Fugitive File - validated by the Royal Canadian Mounted Police (RCMP) for foreign fugitive records entered by RCMP, or Interpol for foreign fugitive records entered by Interpol (Refer to the Foreign Fugitive File Lesson Plan for more information).

3. Bureau of Alcohol, Tobacco and Firearms Violent Felon File - coordinated with the U.S. Customs Service and validated by the Bureau of Alcohol, Tobacco and Firearms, the entering agency for Alcohol, Tobacco and Firearms violent felon records (Refer to the Alcohol, Tobacco, and Firearms Violent Felon File Lesson Plan for more information).
4. The Vehicle, License Plate, Boat, Gun, Securities, Wanted Person, Missing Person, and Unidentified Person Files are validated by the ORI of the record.
INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA TO DETERMINE VALIDATION RESPONSIBILITY FOR RECORDS ENTERED FOR SERVICED AGENCIES.

III. THE VALIDATION PROCESS

A. NCIC

1. On a monthly basis, the NCIC Communications Center sends each CTA or SC a validation listing (tape, cartridge, or printout) of NCIC records according to the NCIC Validation Schedule. The listing includes all records entered into NCIC by the agency or agencies under the CTA or SC's jurisdiction.
2. Included with each validation listings are two letters which must be signed and returned by the CTO or SC.
 - (a) The acknowledgement letter is used to acknowledge receipt of the validation materials. This letter should be returned immediately.
 - (b) The certification letter is used to certify that all records on the listing have been validated. This letter must be returned within 45 days of receipt.

HD #1

HD #2,3

3. The NCIC Communications Center monitors the return of both letters. The acknowledgement letter is monitored to ensure that the validation listings are received by the CTO or SC. The certification letter is monitored to ensure the return of the certification letter within the allotted time.

B. The CTO or SC

IO #4

1. The CTO or SC receives the validation listings from NCIC. The acknowledgement letter should be returned immediately.
2. The CTO or SC disseminates the validation listings to the appropriate agencies for certification.
3. The CTO or SC is then responsible for ensuring that the validating agencies certify their records and return the certification documents within the allotted time.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA OR SC TO DETERMINE THE DEADLINE FOR COMPLETING AND RETURNING THE VALIDATION LISTINGS.

C. The Validating Agency

IO #5
OH #3

The Originating Agency Identifier (ORI) of each NCIC record is responsible for the validation of that record. Terminal agencies that enter NCIC records for other agencies may be responsible for the validation of the serviced agencies' records either by CTA policy or by written agreement between the terminal and serviced agencies.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA TO DETERMINE VALIDATION RESPONSIBILITY FOR RECORDS ENTERED FOR SERVICED AGENCIES.

1. The validating agency, upon receipt of the validation listing from the CTO or SC, must compare every record on the listing against supporting documentation such as case files, incident reports, and warrants to ensure accuracy, validity, and completeness of the data entered in the NCIC record.

2. A second step is necessary for validation of wanted person, vehicle, and missing person records. To ensure validity of the NCIC record, the validating agency is required to make a recent consultation with the prosecutor or court with respect to the wanted person records and with the complainant, victim, motor registry files, or other appropriate source or individual with regards to vehicle and missing person records.

- (a) Recent consultation to the prosecutor or court for wanted person records can be accomplished by:

IO #6

1. telephone call
2. personal visit
3. letter or memorandum to the courts or prosecutor
4. access to a court computer system updated only by the courts
5. letter, memorandum, or printout from the court or prosecutor identifying active warrants.

- (b) Recent consultation to the appropriate individual for vehicle records can be accomplished by:

HD #4

1. telephone call
2. personal visit
3. letter or postcard.

INSTRUCTOR'S NOTE: SOME AGENCIES HAVE IN-HOUSE COMPUTER SYSTEMS WHICH GENERATE VEHICLE VALIDATION LETTERS OR POSTCARDS COMPLETE WITH THE NECESSARY INFORMATION.

- (c) Recent consultation to the appropriate individual for missing person records can be accomplished by:

1. telephone call
2. personal visit
3. letter or postcard.

INSTRUCTOR'S NOTE: DUE TO THE SENSITIVITY OF MISSING PERSON CASES, AGENCIES USUALLY PREFER TO HAVE THE INVESTIGATORS ASSIGNED

7/1/92

VAL-10

TO THE CASE COMPLETE THE RECENT
CONSULTATION FOR MISSING PERSON RECORDS.

Consultation is essential for proper validation of the Wanted Person, Vehicle, and Missing Person Files. NCIC audits have noted occasions where courts or prosecutors have failed to notify the validating agencies when warrants have been dismissed or served. NCIC audits have also determined that reporting parties often fail to notify the validating agencies when the vehicle or missing person has been found or located.

Remember that if the reporting party, court, or prosecutor failed to notify the validating agency of the return of the missing person, dismissal of the warrant, etc., the ORI of the record is still responsible for the consequences of the record in NCIC. Recent consultation is an effective means of ensuring that invalid records are removed from NCIC.

3. In the event the validating agency cannot make such a contact, a decision must be made by appropriate personnel within the validating agency whether to retain the record in the NCIC File.
4. Additionally, it is suggested that during validation of wanted person records, the agency:
 - (a) check with the Interstate Identification Index (III) and state and local criminal history systems for additional descriptors that may be added to the NCIC record.
 - (b) confirm the validity of the extradition with the appropriate source.
 - (c) check, if extradition limitations were unknown at the time of entry, with the appropriate source for any subsequent extradition limitations.

For vehicle records, it is suggested that the agency:

- (a) check with the state agency responsible for motor vehicle registration to confirm license and vehicle information.
 - (b) check the accuracy of the Vehicle Identification Number (VIN) with the National Insurance Crime Bureau (NICB) manuals.
5. When an agency completes the validation process, a certification document must be signed and returned to the CTO or SC.

The validation process described above is the minimum standard that has been established by NCIC. Your CTA or SC may have additional requirements. Consult your state operating manual or CTA for more information.

V. VALIDATION CERTIFICATION

IO #7
OH #4

A signed certification letter from either the CTO, SC, or validating agency indicates that:

- (a) The records on the validation listing have been reviewed.
- (b) The records which are no longer current have been removed and all remaining records are valid and active.
- (c) All records contain all available information.
- (d) The information contained in each record is accurate.

If an agency fails to properly validate its records or does not return the certification letter, the state or NCIC will purge that agency's

7/1/92

VAL-12

unvalidated records. If a CTO or SC fails to return the certification letter, the CTO or SC will be subject to sanctions from the Advisory Policy Board (Refer to the NCIC Standards and Sanctions Lesson Plan).

V. VALIDATION DOCUMENTATION

Validation procedures must be developed and made available to all personnel involved in the process. Failure to formalize and distribute validation procedures to the necessary personnel may result in the agency's records not being properly validated.

Documentation of the validation process, including recent consultation, should be retained by the validating agency. The documentation may prove valuable in a later lawsuit alleging that the validating agency failed to follow proper procedures.

HD #5

Validation procedures and documentation are assessed in NCIC Audits. Failure to have either procedures or documentation will result in a higher risk assessment of the agency by the NCIC Audit Staff.

VI. CONCLUSION

OH #5

7/1/92

VAL-13

Validation is the primary tool for ensuring that an NCIC record is complete, accurate, and outstanding. It is particularly important to remember:

- A. Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active.
- B. Validation is accomplished by:
 - 1. Reviewing the record against supporting documentation.
 - 2. Recent consultation with the appropriate source for wanted person, vehicle, and missing person records.
- C. Validation certification means the records have been reviewed, contain all available information, the information is accurate, and the records which are no longer current are removed from NCIC.
- D. Unvalidated records will be purged from NCIC.

Valid, accurate, and complete records are essential to the effective use of NCIC. Accurate information in NCIC not only informs the officer of the potential dangers faced in the line of duty, but also ensures that innocent citizens are not subjected to false arrest.

SHOW NCIC
VIDEO

BIBLIOGRAPHY

Austin American Statesman. David Burnham. "False Police Reports." August 25, 1985.

National Automobile Theft Bureau, National Automobile Theft Bureau Manual Palos Hills, Illinois

New York Times. David Burnham. "Computer Data Faulted In Suit Over Wrongful Arrest." January 19, 1986.

U.S. Department of Justice. Federal Bureau of Investigation. National Crime Information Center Operating Manual Washington, D.C. May 31, 1989. Revision 55.

U.S. Department of Justice. Federal Bureau of Investigation "NCIC Audit Staff Vehicle Recontact Letter" Washington, D.C.

U.S. Department of Justice. Federal Bureau of Investigation. NCIC Technical and Operational Update 89-5 Washington, D.C. December 29, 1989.

U.S. Department of Justice. Federal Bureau of Investigation. "NCIC Validation" Video Washington, D.C.

FBI/NCIC

VALIDATIONS

**VALIDATION IS THE PROCESS THROUGH WHICH A VALIDATING
AGENCY CONFIRMS THAT EACH NCIC RECORD IS COMPLETE,
ACCURATE, AND ACTIVE**

VAL-OH #2

VALIDATION IS ACCOMPLISHED BY:

- 1) COMPARISON OF THE NCIC RECORD WITH SUPPORTING DOCUMENTATION SUCH AS CASE FILES OR WARRANTS.**
- 2) RECENT CONSULTATION WITH THE PROSECUTOR, COURTS, COMPLAINANT, VICTIM, MOTOR REGISTRY FILES OR OTHER APPROPRIATE SOURCE FOR THE WANTED PERSON, MISSING PERSON, AND VEHICLE FILE.**

VAL-OH #3

A SIGNED CERTIFICATION LETTER CERTIFIES THAT:

- A) THE RECORDS ON THE VALIDATION LISTING HAVE BEEN REVIEWED.**
- B) THE RECORDS WHICH ARE NO LONGER CURRENT HAVE BEEN REMOVED.**
- C) THE RECORDS CONTAIN ALL AVAILABLE INFORMATION.**
- D) THE INFORMATION CONTAINED IN EACH RECORD IS ACCURATE.**

COURSE SUMMARY

- 1) VALIDATION OBLIGES THE VALIDATING AGENCY TO CONFIRM THE RECORD IS COMPLETE, ACCURATE, AND STILL ACTIVE.**
- 2) VALIDATION IS ACCOMPLISHED BY:**
 - A. REVIEWING THE RECORD AGAINST SUPPORTING DOCUMENTATION.**
 - B. RECENT CONSULTATION WITH THE APPROPRIATE SOURCE FOR THE WANTED PERSON, MISSING PERSON, AND VEHICLE FILE.**
- 3) VALIDATION CERTIFICATION MEANS THE RECORDS HAVE BEEN REVIEWED, CONTAIN ALL AVAILABLE INFORMATION, THE INFORMATION IS ACCURATE, AND THE RECORDS WHICH ARE NO LONGER CURRENT ARE REMOVED.**
- 4) UNVALIDATED RECORDS WILL BE PURGED FROM NCIC.**

VALIDATION SCHEDULE

The validation listing will include any records 60-90 days old, 14-15 months old, 26-27 months old, 38-39 months old according to the following schedule:

Validation Listing Date

January
February
March
April
May
June
July
August
September
October
November
December

Record Entries Included on Listing

October
November
December
January
February
March
April
May
June
July
August
September

NCIC CONTROL TERMINAL
RECEIPT OF VALIDATION MATERIAL

ACKNOWLEDGEMENT

Date: _____

VALIDATION OF RECORDS ENTERED

(MONTH AND YEAR) AND SAME CALENDAR MONTH FOR PRIOR YEARS

As step one of the NCIC Record Validation Certification Program, this letter, which acknowledges receipt of your validation material (magnetic tape, 3480 one-half inch tape cartridge or computer printout listing), should be promptly executed and returned to NCIC Operations.

Step two requires submission of the enclosed Certification Document within 45 days from its date.

Signature
(NCIC Control Terminal Officer)

(NCIC Control Terminal Agency)

Date

VAL-HD #2 339

NCIC CONTROL TERMINAL
VALIDATION CERTIFICATION DOCUMENT

Date: _____

VALIDATION OF RECORDS ENTERED
AND SAME CALENDER MONTH FOR PRIOR YEARS
(MONTH AND YEAR) _____

As the NCIC Control Terminal Officer, I certify that all records received for validation, which were originated in NCIC by this agency, have been validated and/or I have received certification from the originating agencies under this service jurisdiction that they have validated their records. Validation (vehicle, boat, fugitives, and missing person entries) obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation certification means that:

1. The records contained on the validation listing have been reviewed by the originating agencies;
2. The records which are no longer current have been removed from NCIC;
3. All records contain all available information; and
4. The information contained in each of the records is accurate.
5. If a control terminal agency has not received a certification response from an agency under its service jurisdiction within the specified period of time, the control terminal agency shall purge from NCIC all records which are the subject of that agency's validation listing.
6. If a control terminal agency fails to certify any validation listing to the NCIC within the specified time, NCIC shall purge all of the state's unvalidated records.

This document must be signed and returned to NCIC Operations within 45 days from the above date.

Signature
(NCIC Control Terminal Officer)

(NCIC Control Terminal Agency)

Date

To whom it may concern:

Your _____
 was reported stolen or missing to the _____
 Police Department/Sheriff's Office. The stolen vehicle records of this agency are presently being
 reviewed by the National Crime Information Center (NCIC), a nationwide computer network avail-
 able to all law enforcement agencies. This review is being conducted to ensure that the informa-
 tion entered in NCIC is correct and could aid in the recovery of your vehicle.

We ask that you take a minute of your time, answer the questions below, and return the
 form to us. To do so, check the appropriate boxes, re-fold the letter so that the Business Reply ad-
 dress is on the outside, and place the letter in the mail.

Your cooperation is greatly appreciated.

- (1) Have you recovered your vehicle? ☐ Yes ☐ No
- (2) If yes, did you report the return to the ☐ Yes ☐ No
 police department/sheriff's office?

If yes, when did you make the report? _____

- (3) Has ownership of your vehicle been ☐ Yes ☐ No
 transferred to your insurance company?

Answer yes if the insurance company has settled the claim concerning your stolen vehicle.

Please include any comments you may wish to make.

 Signature of Owner

 NIC Number

 OCA Number

 VIN

 YOE

 RAN NUM

 NATB

FBI/DOJ

VAL-HD #4

341

False police reports

FBI study finds abundance of inaccurate crime information

By David Burnham

New York Times Service

WASHINGTON — At least 12,000 invalid or inaccurate reports on suspects wanted for arrest are transmitted each day to law enforcement agencies, according to projections by the Federal Bureau of Investigation.

The estimate of faulty reports was based on a continuing series of FBI audits. The audits also indicated problems with about 7,000 reports transmitted each day concerning stolen vehicles and license plates.

The inaccurate information is provided by thousands of state and local law enforcement agencies to the bureau's National Crime Information Center. The center was established to give police officers notice of whether a person stopped for a traffic offense is wanted on criminal charges in another jurisdiction.

Faulty records are 'a gaping hole' in the criminal justice system.

Rep. Charles E. Schumer

Law enforcement and civil liberties experts say that invalid or false information can endanger the safety of individual officers, the ability of the police to control crime, and the freedom of citizens.

More than 60,000 state and local agencies provide most of the information to the National Crime Information Center, which is now used by law enforcement officers nearly 400,000 times a day.

Dozens of cases have become known in the last few years in which inaccurate information has contributed to the arrest and detention, sometimes for days, of innocent individuals.

Two years ago, for example, Sheila Jackson Stossier, an Eastern Airlines flight attendant, was wrongfully jailed for almost three days in Louisiana on the basis of a Houston arrest warrant that had been placed into the national communications network.

The warrant was for a suspect with a similar name, however, and officials in Louisiana failed to check Miss Stossier's passport and other identity papers that would have shown she was not the person sought.

Rep. Charles E. Schumer, D-N.Y., said the faulty records are "a gaping hole" in the criminal justice system. He has introduced legislation to provide states with federal funds to improve record keeping.

The decision of the FBI to make its audits public marks the first time that the agency has acknowledged the extent of the problem of faulty records.

YOUR SEARCH REQUEST IS:
COMPUTER AND WRONGFUL W/5 ARREST

1ST STORY of Level 1 printed in FULL format.

Copyright (c) 1986 The New York Times Company;
The New York Times

January 19, 1986, Sunday, Late City Final Edition

SECTION: Section 1; Part 1, Page 16, Column 2; National Desk

LENGTH: 843 words

HEADLINE: WRONGFUL ARREST SUIT CITES FLAWS IN COMPUTER DATA

BYLINE: By DAVID BURNHAM, Special to the New York Times

DATELINE: BOSTON, Jan. 15

BODY:

Late one evening last summer a Boston graduate student was arrested at gunpoint and held in jail overnight. A week later he was found not guilty of a crime that never occurred.

The No. 2 official in the Boston Police Department has since acknowledged in a deposition that the department computer that provided the information leading to the arrest contained "quite a few" similarly false reports.

In addition, another senior police official has admitted that the department does not follow the checking procedures mandated by the Federal Bureau of Investigation to assure the accuracy of the information in the computer. His admission, also in a deposition, came after he officially certified to the bureau that such checks were made.

The case began July 9 when John R. Kelly, a Boston police officer, arrested Suke Omere Emma on charges of stealing a family member's car. The car had never been stolen, however, and Mr. Emma was found not guilty. He filed a suit in Federal District Court charging the Police Department with violating his constitutional rights against illegal arrest and imprisonment, saying the department "knowingly and systematically" maintained inaccurate information in its computer.

Thousands of Entries Daily

Armed with the sworn statements of department officials and a critical analysis Boston police procedures by a criminal history expert from New York, Mr. Emma's lawyer, Jeffrey W. Kobrick, asked the court Wednesday to rule that the case be considered an action on behalf of all citizens who might be effected. If this petition is granted by Federal District Judge William A. Young, a victory by Mr. Emma could mean changes in the department's procedures for processing its computer data. Judge Young set a hearing for Jan 22.

Mr. Kobrick said Wednesday that he knew of another similar case. On Nov. 14, 1985, Mr. Kobrick said, Mark L. Juliano was arrested in Boston on the basis of a false stolen car report, held in jail and then found not guilty.

Because much of the information collected by individual police departments like Boston's flows into the National Crime Information Center, a national network maintained by the F.B.I., accuracy problems in one department can plague law-enforcement officials and citizens around the country. suits in Other States

Although similar suits have been brought in Michigan, California and Louisiana, Mr. Emma's challenge is of special interest because of the admission by senior police officials that a significant number of false reports are in the department's computer and that the department has not followed procedures to correct them.

Superintendent-in-Chief John A. Gifford, second in command of the Boston Police Department, said in a recent deposition that the department computer was "still carrying quite a few vehicles as stolen that are not in fact stolen."

Lieut. Paul T. Conway, commanding officer of the department's operations division and the supervisor of the department's computer operations, said in his deposition that the department did not follow the F.B.I.'s regulations requiring periodic checks that "all records remaining in the system are valid and accurate."

Nevertheless, Lieutenant Conway said he had signed letters to the bureau certifying that the record had been reviewed and all those no longer were current had been removed. He said that because of a shortage of personnel only a sampling of records were checked for accuracy.

New York Expert Testifies

Mr. Kobrick also presented a deposition from Adam F. D'Alessandro, a retired computer expert from the New York City Police Department. Mr. D'Alessandro said the statements from the Boston Police Department showed its processing of stolen car reports was "haphazard and highly conducive to serious error."

Michael Bolden, an attorney for the department, said Wednesday that he would have no comment on the case.

Mr. Emma, a 32-year-old graduate student at Northeastern University, was arrested shortly before midnight on July 10 as he was parking the family car in front of his apartment in the Dorchester section. The police handcuffed him, took him to a local stationhouse and charged him with stealing that car, which belonged to Mr. Emma's cousin, Imeutinyan Omere. Although Mr. Emma said that he tried to persuade the officer that the car was not stolen, that he was a close family member of the registered owner of the car, and that his cousin was asleep in the apartment they shared and would verify his story, the police would not listen, he said. .

According to police documents, on Dec. 25, 1984, another member of the Emma family parked the car in an unusual location. Not being able to find the car,

the family went to the local police station and reported it stolen. Several hours later the car was found and the family reported it recovered. The second report, however, was not logged into the Police Department computer. It was this false notice that the gray 1980 Ford was still missing that six months later led to Mr. Emma's arrest.

(c) 1986 The New York Times, January 19, 1986

SUBJECT: Terms not available

DATE: SEPTEMBER 21, 1989

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: SYSTEM SECURITY

TITLE OF INSTRUCTION:

SYSTEM SECURITY

TIME ALLOTTED:

1 HOUR

TARGET GROUP:

FULL ACCESS TERMINAL
OPERATOR

INSTRUCTOR:

METHOD OF INSTRUCTION:

LECTURES, OVERHEAD,
TRANSPARENCIES, AND
VIDEO TAPE PRESENTATION

DATE:

7/1/92

SYSTEM SECURITY LESSON PLAN TABLE OF CONTENTS

	PAGE
STATEMENT OF GOAL AND OBJECTIVES	SS-1
CRITERION TEST	SS-2
CRITERION TEST ANSWERS	SS-4
ITEMS AND MATERIAL	SS-8
INTRODUCTION	SS-9
OVERVIEW OF NCIC	SS-10
NCIC "Hot" Files	SS-10
Interstate Identification Index (III)	SS-10
Obtaining NCIC Information	SS-10
Obtaining III Information	SS-10
USER AUTHORIZATION	SS-11
Originating Agency Identifier (ORI)	SS-11
User Agreements	SS-12
Management Control	SS-12
PHYSICAL SECURITY OF THE NCIC TERMINALS	SS-14
Guidelines for CTAs of FCs	SS-14
PERSONNEL SECURITY	SS-15
TECHNICAL SECURITY	SS-16
Dial-Up Access	SS-16
Logging	SS-16
Requirements for Logging of NCIC Transactions	SS-16
Requirements for Logging of III Transactions	SS-16
DISSEMINATION	SS-16
NCIC Information	SS-16
III	SS-17
III Policies Concerning Storage and Destruction	SS-18
SYSTEM SECURITY ASSESSMENT DURING NCIC AUDITS	SS-19
SANCTIONS FOR MISUSE OF NCIC INFORMATION	SS-20
Penalties for Misuse	SS-20
CONCLUSION	SS-21
BIBLIOGRAPHY	SS-22

STATEMENT OF GOALS AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator critical information on system security including criteria for accessing the system, policies for dissemination, and penalties for misuse of NCIC.

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the operator will:

1. State when NCIC "Hot" File information may be obtained.
2. List the three occasions when III information may be obtained.
3. Be aware that to access NCIC directly, an authorized agency must have an Originating Agency Identifier (ORI).
4. State the NCIC policy regarding user agreements with terminal agencies.
5. List the NCIC policies for physical security.
6. List the NCIC personnel security policies.
7. State the NCIC policy for dial-up access.
8. State when NCIC information may be disseminated.
9. List the NCIC policies regarding dissemination of III information.
10. List the policies regarding III storage and destruction.
11. Describe the penalties for misuse of NCIC information.

CRITERION TEST

OVERVIEW OF NCIC

1. State when NCIC "Hot" File information may be obtained.
2. Describe the three occasions when the Interstate Identification Index (III) may be obtained.

USER AUTHORIZATION

3. NCIC may be accessed directly through a terminal by any authorized criminal justice agency with a valid _____.
4. NCIC requires the CTA or SC to execute user agreements with only criminal justice agencies that access III.
 - A. True.
 - B. False.

PHYSICAL SECURITY

5. State the NCIC policies for physical security of the NCIC terminal.

PERSONNEL SECURITY

6. The revised NCIC personnel security policy now requires submission of a fingerprint card to the FBI Identification Division.
 - A. True.
 - B. False.
7. List the steps that must be taken by the CTA before system access is granted to the operator.

TECHNICAL SECURITY

8. Dial-up access to NCIC and III is allowed in _____ or for _____.

DISSEMINATION OF NCIC INFORMATION

9. NCIC information may be disseminated outside of the criminal justice system for unofficial purposes.
 - A. True
 - B. False

7/1/92

SS-2

DE
11

10. State the NCIC policies regarding III dissemination.
11. State the policies regarding III storage and destruction.

SYSTEM SECURITY ASSESSMENT DURING NCIC AUDIT

12. The CTA or SC may not set security standards stricter than NCIC.
 - A. True
 - B. False
13. NCIC Auditors, during a visit to a randomly selected criminal Justice agency, verify _____ and _____.

SANCTIONS FOR MISUSE OF NCIC INFORMATION

14. Describe the penalties for misuse of NCIC information.

CRITERION TEST ANSWERS

OVERVIEW OF NCIC

1. NCIC "Hot" File information may be obtained for any official criminal justice purpose.
2. III may only be obtained for three reasons:
 - a. III may be obtained in connection with any authorized criminal justice investigation. This includes criminal investigations by law enforcement; pre-sentencing, probation, and parole investigations by courts, and classification and assignment investigations by prisons.
 - b. III may be used in conjunction with a background investigation for criminal justice employment. This includes the investigation of both sworn and nonsworn employees of law enforcement agencies, courts, prisons, and other criminal justice agencies.
 - c. Certain designated Federal agencies, such as the FBI and Department of Defense can use III for background investigations in connection with security clearances.

USER AUTHORIZATION

3. NCIC may be directly accessed through a terminal by any authorized criminal justice agency with a valid Originating Agency Identifier (ORI).
4. False. The NCIC policy on user agreements states:

"Each CTA must prepare and execute a written agreement containing similar provisions to the agreement by the states and NCIC, with each criminal justice agency having a terminal device capable of accessing NCIC and III data within the state."

PHYSICAL SECURITY

5. NCIC policy requires for any terminal that accesses NCIC or III:
 - a. "The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data."

- b. "All visitors to computer centers and/or terminal areas must be accompanied by staff personnel at all times."
- c. "Agencies having terminals with access to NCIC and III information must have terminal operators screened according to specified guidelines. Access to the terminal area should also be restricted to the minimum number of authorized employees needed to complete the work."

PERSONNEL SECURITY

6. True. The policy states:

"Appropriate background investigations must be conducted on all NCIC terminal operators, including submission of a completed applicant fingerprint card to the FBI Identification Division through the state identification Bureau.

7. The steps that must be taken by the CTA before system access is granted are:

- a. The CTA and/or the employing agency staff must check state and national arrest and fugitive files.
- b. If a record of any kind is found, access will not be granted. The agency to which the applicant has applied for employment and/or NCIC access will be formally notified indicating NCIC access will be delayed pending review of arrest and fugitive records.
- c. When identification of the applicant has been established by fingerprint comparison and he/she appears to be a fugitive or to have an arrest history for a felony or serious misdemeanor, the matter will be referred to the agency head or their designee will review the matter. If the applicant is found to be a fugitive from justice, or to have been convicted of a felony or serious misdemeanor, the matter will be referred to the executive head of the CTA or his/her designee.
- d. If a determination is made that NCIC access by the applicant would not be in the public interest, such access will be denied and the applicant's appointing authority will be notified in writing of the access denial."

TECHNICAL SECURITY

7/1/92

SS-5

8. Dial-up access to NCIC and III is allowed in emergency situations or for CTA diagnostic purposes.

DISSEMINATION OF NCIC INFORMATION

9. False. NCIC information may not be disseminated outside of the criminal justice system without an official purpose.
10. The NCIC policies regarding III dissemination are:
- a. "Due to variance in state laws and policies, the III cannot be used for licensing or noncriminal justice employment purposes." (NCIC OM, 10-25, Para 3.1) (11-1-87)
 - b. "The III shall not be used for remotely accessing a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing either to the FBI Identification Division or state of record." (III OTM, Intro-6) (7-1-91)
 - c. "Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data." (NCIC OM, 10-20, Para VII (C-3) (11-17-86)
 - d. "Each criminal justice agency receiving an III response shall record any secondary dissemination of any III response to another criminal justice agency or an individual within another agency, or to anyone legally entitled to receive such information who is outside the original receiving agency. These logs shall be maintained for at least 12 months. (Advisory Policy Board Minutes, Page 310) (10-84)
 - e. "Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the transmission of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. When an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public, then details of criminal history may be transmitted. (NCIC OM, 10-20, Para VII (B-3)
11. The policies regarding III storage and destruction are:

- a. "III records be maintained in a secure records environment. Such storage of records will be retained for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal records files where they are retained."
- b. "When retention of III records is no longer required, final disposition will be accomplished in a secure manner so as to preclude unauthorized access/use."

SYSTEM SECURITY ASSESSMENT DURING NCIC AUDITS

- 12. False. NCIC standards, at the minimum, must be met; however, the CTA or SC may set stricter standards.
- 13. NCIC auditors, during a visit to a randomly selected criminal Justice agency, verify 1) compliance with NCIC policies and 2) effectiveness of CTA or SC system controls over local agencies.

SANCTIONS FOR MISUSE OF NCIC INFORMATION

- 14. The penalties for misuse of NCIC are:
 - a. Administrative sanctions taken against an agency for failing to ensure that employees comply with rules concerning dissemination of NCIC information.
 - b. Termination of NCIC services if violations continue.
 - c. Criminal penalties for those individuals who profit from misuse of NCIC information.

ITEMS AND MATERIALS:

Overhead Projector and Screen

Overhead Transparencies:

- SS-OH #1 - System Security
- SS-OH #2 - The Two Types of NCIC Information
- SS-OH #3 - NCIC "Hot" File Information Use
- SS-OH #4 - Permitted Uses of III
- SS-OH #5 - NCIC Availability
- SS-OH #6 - When Management Control is Required
- SS-OH #7 - Physical Security Requirements
- SS-OH #8 - Personnel Security Requirements
- SS-OH #9 - Dissemination of NCIC Information
- SS-OH #10 - NCIC Policies for Storage and Destruction of III
- SS-OH #11 - Sanctions for Misuse of NCIC Information
- SS-OH #12 - Course Summary

Handouts:

- SS-HD #1 - SCIA Act
- SS-HD #2 - Example of a Management Control Agreement
- SS-HD #3 - NCIC Policies Regarding III Access and Dissemination
- SS-HD #4 - NCIC Audit Staff Security Compliance Checklist
- SS-HD #5 - Newspaper Clippings

VCR and Monitor

Video:

System Security

I. INTRODUCTION

The NCIC System consists of the following: the NCIC computer, agencies that access NCIC, the personnel within the agencies who utilize the NCIC System, NCIC terminals, and the information contained in the NCIC Files.

The FBI, in conjunction with state Control Terminal Agencies (CTA) and Service Coordinator (SC), use hardware and software controls to help ensure security of the NCIC System. However, final responsibility for the maintenance of the security and confidentiality of NCIC information rests with the individual utilizing the NCIC System.

In 1992, the Advisory Policy Board (APB) revised and instituted a number of the NCIC System security policies. This lesson plan will provide the revised and existing policies. Information regarding CTA and SC system security requirements are also presented to provide a thorough overview of NCIC System Security.

Effective use of this lesson plan will help local agency personnel to ensure security for the NCIC terminal(s) and information within their agency.

References

IO =
Instruc-
tional
Objectives

OH =
Overhead
Transp-
arencies

OH #1

HD =
Handouts

NCIC OM =
NCIC
Operating
Manual

III OTM =
III
Operating,
Technical
Manual

7/1/92

SS-9

b₁

II. OVERVIEW OF NCIC

OH #2

There are two types of NCIC information:

1. "Hot" Files - consists of the: Vehicle, License Plate, Boat, Gun, Article, Securities, Wanted Person, Foreign Fugitive, United States Secret Service Protective, Missing Person, Unidentified Person, and the Bureau of Alcohol, Tobacco and Firearms Files.
INSTRUCTOR'S NOTE: REFER TO THE RESPECTIVE "HOT" FILE LESSON PLAN FOR MORE INFORMATION.
2. Interstate Identification Index (III) - contains records for offenders of serious and or significant violations that are 1) known to the FBI, 2) with a date of birth of 1956 or later, or 3) arrested for the first time and reported to the FBI Identification Division since July 1, 1974 (regardless of date of birth). III information is considered extremely sensitive.
INSTRUCTOR'S NOTE: REFER TO THE III LESSON PLAN FOR MORE INFORMATION.

NCIC "Hot" File information may be obtained for any official criminal justice purpose.

IO #1

OH #3

III may be obtained for three reasons:

IO #2

1. III may be obtained in connection with any authorized criminal justice investigation. This includes criminal investigations by law enforcement; pre-sentencing, probation, and parole investigations by courts, and classification and assignment investigations by prisons.
2. III may be used in conjunction with a background investigation for criminal justice employment. This includes the investigation of both sworn and nonsworn employees of law enforcement agencies, courts, prisons, and other criminal justice agencies.
3. Certain designated Federal agencies, such as the FBI and Department of Defense can use III for background investigations in connection with security clearances.

OH #4

HD #1

III. USER AUTHORIZATION

NCIC is confidential information and is accessible only to authorized criminal justice agencies. User access to NCIC is controlled through a number of technical and administrative requirements.

OH #5

A. Originating Agency Identifier (ORI)

System access is controlled through assignment and use of ORI. Any agency directly accessing NCIC through a terminal, must have a valid ORI.

IO #3

Agencies desiring direct access to NCIC information, must apply for an ORI through their CTA or SC. The CTA or SC approves all ORI requests, determines level of access, and forwards all ORI requests to NCIC for ORI assignment.

To ensure compliance with NCIC ORI policies, the APB instituted the following:

"The ORI must be used in each transaction on the System, and thereby serve to ensure the proper level of access in each transaction. At the initial submission of a transaction into the System, the ORI is automatically referenced to the relevant state telecommunication circuit. The CTA must further ensure that the ORI is in fact originating from the assigned location(s) within the state. This will prevent one agency from masquerading as another. Additionally, this will ensure that an agency wishing to modify or cancel an NCIC entry is the entering agency."

INSTRUCTOR'S NOTE: PASSWORDS, LOGONS, ETC., MAY ALSO BE REQUIRED TO ACCESS NCIC IN SOME STATE SYSTEMS. CHECK WITH YOUR CTO OR SC FOR MORE INFORMATION.

B. User Agreements

An NCIC User agreement must be signed between each CTA and NCIC. The user agreement includes the following language:

"An agency participating in the NCIC as a CTA and other agencies with direct telecommunications line access must assume responsibility for and enforce NCIC System security with regard to all other agencies which it, in turn, services."

To ensure compliance of NCIC policies by the local agencies, NCIC requires the CTA to execute user agreements with each criminal justice agency under its jurisdiction. The policy states:

"Each CTA must prepare and execute a written agreement containing similar provisions to the agreement by the states and NCIC, with each criminal justice agency having a terminal device capable of accessing NCIC and III data within the state."

IO #4

"Each terminal agency must also prepare and execute, in the absence of such an agreement with the CTA, a written agreement, approved by the CTA, for each nonterminal agency for whom they provide NCIC and III service which contains similar provisions to the agreement between the terminal agency and the CTA."

INSTRUCTOR'S NOTE: THIS POLICY HAS BEEN REVISED TO INCLUDE ALL AGENCIES THAT ACCESS NCIC THROUGH THE CTA OR SC. PREVIOUSLY, NCIC HAD ONLY REQUIRED THE CTA OR SC TO EXECUTE WRITTEN AGREEMENTS WITH CRIMINAL JUSTICE AGENCIES ACCESSING III.

C. Management Control

NCIC policy requires:

"All computers, electronic switches, and manual terminals interfaced directly with the interface computer for the interstate exchange of criminal history information

must be under the management control of criminal justice agencies." (NCIC OM, 10-15, 10-16, PARA IV) (11-17-86).

Management control is defined as the authority by a criminal justice agency to set:

- 1) priorities, 2) standards for the selection, supervision, and termination of personnel; and
- 3) policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit criminal history record information over a noncriminal justice agency accessing III.

Management control is required for:

OH #6

1. Noncriminal justice (e.g., county or city) interfaces or message switchers where III passes through to other agencies (even though the interface or message switchers do not access it),
2. Noncriminal justice communication/dispatch/911 centers.

Any noncriminal justice entity accessing III must be under the management control of a criminal justice agency. The criminal justice agency must have a written agreement with the noncriminal justice agency assuring that the criminal justice agency has management control as defined above.

HD #2

INSTRUCTOR'S NOTE: YOUR CTA MAY HAVE ADDITIONAL REGULATIONS CONCERNING MANAGEMENT CONTROL. CONSULT YOUR CTA FOR MORE INFORMATION.

INSTRUCTOR'S NOTE: NO CHANGES WERE MADE TO THE MANAGEMENT CONTROL POLICY.

7/1/92

SS-13

Fig.

IV. PHYSICAL SECURITY

An important aspect of system security includes ensuring that the NCIC terminal is afforded proper security. NCIC policy states:

IO #5

OH #7

1. "The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data."
2. "All visitors to computer centers and/or terminal areas must be accompanied by staff personnel at all times."
3. "Agencies having terminals with access to NCIC and III information must have terminal operators screened according to specified guidelines. Access to the terminal area should be restricted to the minimum number of authorized employees needed to complete the work."

In addition, the Advisory Policy Board has developed the following guidelines for physical security:

1. CTAs should have procedures in place to monitor all security policies, e.g., through Terminal Agency Coordinators, state audit programs, etc.
2. Operators should use the terminal only for those purposes for which they are authorized.
3. CTAs should have procedures in place regarding changing of passwords, logons, etc., in relation to terminated employees.

INSTRUCTOR'S NOTE: THIS POLICY HAS BEEN REVISED TO INCLUDE TERMINALS THAT ACCESS NCIC "HOT" FILE. PREVIOUSLY, NCIC HAD ONLY REQUIRED SECURITY FOR TERMINAL THAT ACCESSED III.

V. PERSONNEL SECURITY

System security includes ensuring that the operators, programmers, and other persons employed to utilized or access the NCIC System should be thoroughly screened.

NCIC policy states:

IO #6

"Appropriate background investigations must be conducted on all NCIC terminal operators, including submission of a completed applicant fingerprint card to the FBI Identification Division through the state identification Bureau. When a request for operator access to NCIC is received by the CTA, before system access is granted:

1. The CTA and/or the employing agency staff must check state and national arrest and fugitive files.
2. If a record of any kind is found, access will not be granted. The agency to which the applicant has applied for employment and/or NCIC access will be formally notified indicating NCIC access will be delayed pending review of arrest and fugitive records.
3. When identification of the applicant has been established by fingerprint comparison and he/she appears to be a fugitive or to have an arrest history for a felony or serious misdemeanor, the matter will be referred to the agency head or their designee will review the matter. If the applicant is found to be a fugitive from justice, or to have been convicted of a felony or serious misdemeanor, the matter will be referred to the executive head of the CTA or his/her designee.
4. If a determination is made that NCIC access by the applicant would not be in the public interest, such access will be denied and the applicant's appointing authority will be notified in writing of the access denial."

INSTRUCTOR'S NOTE: REVISED NCIC POLICY NOW

OH #8

7/1/92

SS-15

REQUIRES FINGERPRINT SUBMISSIONS TO THE FBI IDENTIFICATION DIVISION AND OTHER PERSONNEL SECURITY MEASURES FOR EMPLOYEES THAT ACCESS NCIC. PREVIOUSLY, BACKGROUND CHECKS WERE REQUIRED ONLY REQUIRED FOR EMPLOYEES WHO ACCESS III. FINGERPRINT SUBMISSIONS TO THE FBI IDENTIFICATION WAS NOT REQUIRED AS WELL.

VI. TECHNICAL SECURITY

A. Dial-Up Access

IO #7

Dial-up access is the process of accessing computer information using nondedicated telephone communications. Dial-up access to NCIC and III information is allowed in emergency situations or for CTA diagnostic purposes.
INSTRUCTOR'S NOTE: THE NCIC POLICY FOR DIAL-UP ACCESS HAS NOT CHANGED.

B. Logging

NCIC policy requires the CTAs and SCs to maintain an automated log of:

1. all "Hot" File transactions for a minimum of 6 months,
and
2. all "III" transactions (both QH index inquiry and QR record request) for a minimum of one year. The log must in some way identify the operator, requestor, and authorizing agency.

INSTRUCTOR'S NOTE: THIS POLICY HAS BEEN REVISED TO INCLUDE LOGGING OF ALL "HOT" FILE TRANSACTIONS. PREVIOUSLY, CTAs AND SCs WERE ONLY REQUIRED TO LOG III TRANSACTIONS.

VII. DISSEMINATION OF NCIC INFORMATION

A. NCIC Dissemination

7/1/92

SS-16

P. P.

The information available through NCIC is documented criminal justice information. This information must be protected to ensure correct, legal, and efficient dissemination.

NCIC information may be disseminated to any criminal justice professional in conjunction with an official purpose. This includes authorized personnel in criminal justice agencies that do not have an NCIC terminal (nonterminal agencies). However, NCIC information may not be disseminated outside of the criminal justice system without an official purpose.

B. III Dissemination

Due to the highly sensitive nature of III information, NCIC has established specific policies that must be followed by criminal justice agencies in accessing and disseminating III information:

1. "Due to variance in state laws and policies, the III cannot be used for licensing or noncriminal justice employment purposes." (NCIC OM, 10-25, Para 3.1) (11-1-87)
2. "The III shall not be used for remotely accessing a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing either to the FBI Identification Division or state of record." (III OTM, Intro-6) (7-1-91)
3. "Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data." (NCIC OM, 10-20, Para VII (C-3) (11-17-86)

IO #8

OH #9

IO #9

HD #3

7/1/92

SS-17

4. "Each criminal justice agency receiving an III response shall record any secondary dissemination of any III response to another criminal justice agency or an individual within another criminal justice agency, or to anyone legally entitled to receive such information who is outside the original receiving agency. These logs shall be maintained for at least 12 months." (Advisory Policy Board Minutes, Page 310) (10-84)
5. "Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the transmission of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. When an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public, then details of criminal history may be transmitted." (NCIC OM, 10-20, Para VII (B-3))

Recently, the APB instituted the following policies concerning III storage and destruction:

1. "III records be maintained in a secure records environment. Such storage of records will be retained for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal records files where they are retained."
2. "When retention of III records is no longer required, final disposition will be accomplished in a secure manner so as to preclude unauthorized access/use."

INSTRUCTOR'S NOTE: THESE ARE NEW POLICIES REGULATING THE STORAGE AND DESTRUCTION OF III.

INSTRUCTOR'S NOTE: A FACSIMILE MACHINE MAY BE USED TO TRANSMIT III INFORMATION PROVIDED THAT BOTH AGENCIES INVOLVED HAVE AN ORIGINATING AGENCY IDENTIFIER (ORI) AUTHORIZED TO RECEIVE CRIMINAL HISTORY INFORMATION. AS NOT ALL FACSIMILE MACHINES ARE MONITORED CONTINUALLY, THE RECEIVING AGENCY SHOULD BE NOTIFIED PRIOR

IO #10

OH #10

TO TRANSMITTING THE INFORMATION. THIS WILL ENSURE PROPER RETRIEVAL OF INFORMATION.

INSTRUCTOR'S NOTE: MANY STATE AND LOCAL SYSTEMS HAVE ADDITIONAL REGULATIONS CONCERNING THE USE OF CRIMINAL HISTORY FILES. CONSULT YOUR STATE CONTROL TERMINAL OFFICER AND STATE SYSTEM OPERATING MANUAL FOR MORE INFORMATION.

VIII. SYSTEM SECURITY ASSESSMENT DURING NCIC AUDITS

System security is assessed during the biennial NCIC Audit of each CTA or SC. Compliance with system security policies is initially assessed at the CTA or SC. NCIC auditors, during the CTA or SC audit, determine the personnel security, terminal security, and dissemination policies that must be followed by criminal justice agencies within the jurisdiction of the CTA or SC. NCIC standards, at the minimum, must be met. However, the CTA or SC may set stricter standards.

NCIC auditors then visit randomly selected criminal justice agencies within the jurisdiction of the CTA or SC. During the visit, the NCIC auditors verify:

1. compliance with NCIC policies,
2. effectiveness of CTA or SC system controls over local agencies.

Any areas of noncompliance will be noted by the auditors and reported to the CTA or SC for follow-up action. Continued noncompliance with NCIC policy may result in sanctions imposed by the CTA or SC.

7/1/92

SS-19

HD #4

IX. SANCTIONS FOR MISUSE OF NCIC INFORMATION

Misuse of NCIC information can have severe repercussions. Careless misuse of NCIC, such as operating the NCIC terminal in a open, public area can compromise cases, violate the privacy of citizens, and destroy reputations. Intentional misuse, such as accepting money or favors in exchange for NCIC information, can violate criminal statutes. The penalties for misuse of NCIC are:

1. Administrative sanctions taken against an agency for failing to ensure that employees comply with rules concerning dissemination of NCIC information.
2. Termination of NCIC services if violations continue.
3. Criminal penalties for those individuals who profit from misuse of NCIC information.

The APB instituted a policy that requires:

"Each criminal justice agency authorized to receive NCIC information must have appropriate written standards for discipline of NCIC policy violators."

INSTRUCTOR'S NOTE: THE APB ALSO RECOMMENDED MISUSE OF THE NCIC SYSTEM SHOULD INCLUDE IMPROPER ALTERATION OF RECORDS.

INSTRUCTOR'S NOTE: REFER TO THE NCIC STANDARDS AND SANCTIONS LESSON PLAN FOR MORE INFORMATION.

X. CONCLUSION

In accessing NCIC, it is particularly important to remember:

7/1/92

SS-20

IO #11

OH #11

HD #5

OH #12

1. NCIC is criminal justice information.
2. NCIC may be used only by criminal justice employees.
3. NCIC may only be used for specified criminal justice purposes.
4. Intentional misuse of NCIC may be punishable by criminal sanctions.
5. Key NCIC User Authorization, Physical, Personnel, and Technical Policies have been revised.

Effective utilization of the guidelines presented in this lesson plan will help ensure that the correct procedures are followed in the use, access, and dissemination of NCIC information.

INSTRUCTOR'S NOTE: SHOW THE NCIC VIDEO "SYSTEM SECURITY."

BIBLIOGRAPHY

Federal Bureau of Investigation, The FBI Identification Division, Washington, D.C. Interstate Identification Index Operational and Technical Manual July 1, 1991.

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. NCIC Audit Staff Manual, April 1991.

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. NCIC Operating Manual May 31, 1989, Revision 55.

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. "System Security" Video.

The Washington Post, "18 Charged With Lifting U.S. Computer Data." 12/12/91.

The Washington Post, "Theft of U.S. Data Seen as Growing Threat to Privacy," by Michael Isikoff.

The Washington Times, "Private Info Sold By Ring, FBI Says," by Jerry Seper.

SYSTEM SECURITY

THE TWO TYPES OF NCIC INFORMATION

1) "HOT" FILES - WHICH CONSIST OF:

VEHICLE
LICENSE PLATE
BOAT
GUN
ARTICLE
SECURITIES
WANTED PERSON
FOREIGN FUGITIVE
UNITED STATES SECRET SERVICE PROTECTIVE
MISSING PERSON
UNIDENTIFIED PERSON
BATF VIOLENT FELON

2) INTERSTATE IDENTIFICATION INDEX (III) - WHICH CONTAINS RECORDS FOR OFFENDERS OF SERIOUS AND OR SIGNIFICANT VIOLATIONS THAT ARE 1) KNOWN TO THE FBI, 2) WITH A DATE OF BIRTH OF 1956 OR LATER, OR 3) ARRESTED FOR THE FIRST TIME AND REPORTED TO THE FBI IDENTIFICATION DIVISION SINCE JULY 1, 1974.

**NCIC "HOT" FILE INFORMATION MAY BE OBTAINED FOR
ANY OFFICIAL CRIMINAL JUSTICE PURPOSE.**

PERMITTED USES OF III

III MAY OBTAINED FOR THREE REASONS:

- 1) III MAY BE OBTAINED IN CONNECTION WITH ANY AUTHORIZED CRIMINAL JUSTICE INVESTIGATION.**
- 2) III MAY BE USED IN CONJUNCTION WITH A BACKGROUND INVESTIGATION FOR CRIMINAL JUSTICE EMPLOYMENT.**
- 3) III MAY BE USED BY CERTAIN DESIGNATED FEDERAL AGENCIES, SUCH AS THE FBI AND DEPARTMENT OF DEFENSE FOR BACKGROUND INVESTIGATIONS IN CONNECTION WITH SECURITY CLEARANCES.**

NCIC IS AVAILABLE ONLY TO AUTHORIZED CRIMINAL
JUSTICE AGENCIES.

WHEN MANAGEMENT CONTROL IS REQUIRED

MANAGEMENT CONTROL IS REQUIRED FOR:

- 1. NONCRIMINAL JUSTICE (e.g., COUNTY OR CITY) INTERFACES MESSAGE SWITCHERS WHERE III PASSES THROUGH TO OTHER AGENCIES (EVEN THOUGH THE INTERFACE OR MESSAGE SWITCHERS DO NOT ACCESS IT),**
- 2. NONCRIMINAL JUSTICE COMMUNICATION/DISPATCH/911 CENTERS.**

PHYSICAL SECURITY REQUIREMENTS

NCIC POLICY REQUIRES THE FOLLOWING FOR ANY TERMINAL THAT ACCESSES NCIC OR III:

- 1. "THE COMPUTER SITE AND/OR TERMINAL AREA MUST HAVE ADEQUATE PHYSICAL SECURITY TO PROTECT AGAINST ANY UNAUTHORIZED PERSONNEL GAINING ACCESS TO THE COMPUTER EQUIPMENT OR TO ANY OF THE STORED DATA."**
- 2. "ALL VISITORS TO COMPUTERS CENTERS AND/OR TERMINAL AREAS MUST BE ACCOMPANIED BY STAFF PERSONNEL AT ALL TIMES."**
- 3. "AGENCIES HAVING TERMINALS WITH ACCESS TO NCIC AND III INFORMATION MUST HAVE TERMINAL OPERATORS SCREENED ACCORDING TO SPECIFIED GUIDELINES. ACCESS TO THE TERMINAL AREA SHOULD BE RESTRICTED TO THE MINIMUM NUMBER OF AUTHORIZED EMPLOYEES NEEDED TO COMPLETE THE WORK. "**

PERSONNEL SECURITY REQUIREMENTS

**REVISED NCIC POLICY NOW REQUIRES FINGERPRINT
SUBMISSIONS TO THE FBI IDENTIFICATION DIVISION AND
OTHER PERSONNEL SECURITY MEASURES FOR
EMPLOYEES THAT ACCESS NCIC.**

**NCIC INFORMATION MAY BE DISSEMINATED TO ANY CRIMINAL
JUSTICE PROFESSIONAL IN CONJUNCTION WITH AN
OFFICIAL PURPOSE.**

NCIC POLICIES FOR STORAGE AND DESTRUCTION OF III INFORMATION

- 1. "III RECORDS BE MAINTAINED IN A SECURE RECORDS ENVIRONMENT. SUCH STORAGE OF RECORDS WILL BE RETAINED FOR EXTENDED PERIODS ONLY WHEN THE III RECORDS ARE KEY ELEMENTS FOR THE INTEGRITY/UTILITY OF THE CASE FILES/CRIMINAL RECORDS FILES WHERE THEY ARE RETAINED."**
- 2. "WHEN RETENTION OF III RECORDS IN NO LONGER REQUIRED, FINAL DISPOSITION WILL BE ACCOMPLISHED IN A SECURE MANNER SO AS TO PRECLUDE UNAUTHORIZED ACCESS/USE."**

SANCTIONS FOR MISUSE OF NCIC INFORMATION

THE PENALTIES FOR MISUSE OF NCIC ARE:

- 1) ADMINISTRATIVE SANCTIONS TAKEN AGAINST AN AGENCY FOR FAILING TO ENSURE THAT EMPLOYEES COMPLY WITH RULES CONCERNING DISSEMINATION OF NCIC INFORMATION.**
- 2) TERMINATION OF NCIC SERVICES IF VIOLATIONS CONTINUE.**
- 3) CRIMINAL PENALTIES FOR THOSE INDIVIDUALS WHO PROFIT FROM MISUSE OF NCIC INFORMATION.**

COURSE SUMMARY

IN ACCESSING NCIC, IT IS PARTICULARLY IMPORTANT TO REMEMBER:

- 1. NCIC IS CRIMINAL JUSTICE INFORMATION.**
- 2. NCIC MAY BE USED ONLY BY CRIMINAL JUSTICE EMPLOYEES.**
- 3. NCIC MAY ONLY BE USED FOR SPECIFIED CRIMINAL JUSTICE PURPOSES.**
- 4. INTENTIONAL MISUSE OF NCIC MAY BE PUNISHABLE BY CRIMINAL SANCTIONS.**
- 5. KEY NCIC USER AUTHORIZATION, PHYSICAL, PERSONNEL, AND TECHNICAL POLICIES HAVE BEEN REVISED.**

5 § 8913

Notes

claim upon which relief could be granted since U.S. was not proper party to suit for benefits of such type. Director, Edward J. Meyer Memorial Hospital v. Setz, D.C.N.Y. 1977, 433 F.Supp. 323.

Where applicable statutes and regulations could not be read as specifically directing employing federal officials to classify employees at issue as something other than "temporary," "term" or "intermittent" employees, such parties did not have substantive right to be classified as other than "temporary" or "intermittent," so as to have right to monetary equivalent of annual and sick leave benefits, as well as health and life insurance benefits. Anderson v. U.S., 1984, 5 Cl.Ct. 573, affirmed 764 F.2d 849.

7. Removal of action

Where neither federal question nor diversity jurisdiction could be asserted with respect to suit brought by hospital director to claim amounts allegedly owed by federal employee as result of his wife's hospitalization or to employee's third-party claim against national association of letter carriers seeking to recover health benefits, and where concurrent third-party claim against Commission,

MENT ORGANIZATION

which resulted in petition for removal of case from Buffalo City Court, was barred by section 2480 of Title 28 because it was based upon misrepresentation, original claim and remaining third-party claim would be remanded to Buffalo City Court for further determination. Director, Edward J. Meyer Memorial Hospital v. Setz, D.C. N.Y. 1977, 433 F.Supp. 323.

8. Review

Federal regulation stating that federal employees' health benefits policy claimant "may" seek review by OPM does not dispense with requirement of exhaustion of administrative remedies. Bauman v. Blue Cross-Blue Shield of Alabama, D.C.Ala. 1984, 579 F.Supp. 265.

The Office of Personnel Management did not act arbitrarily or capriciously when it refused to order carrier to pay benefits pursuant to plan created under this chapter to cover costs incurred by hospitalization of plaintiff's son, since the Office considered relevant factors and did not make a clear error of judgment. Levin v. Connecticut Blue Cross, Inc., D.C.M. 1980, 487 F.Supp. 385.

§ 8914. Effect of other statutes

Any provision of law outside of this chapter which provides coverage or any other benefit under this chapter to any individuals who (based on their being employed by an entity other than the Government) would not otherwise be eligible for any such coverage or benefit shall not apply with respect to any individual appointed, transferred, or otherwise commencing that type of employment on or after October 1, 1988.

(Added Pub.L. 100-238, Title I, § 106(a)(3)(A), Jan. 8, 1988, 101 Stat. 1747.)

Historical and Statutory Notes

Legislative History. For legislative history and purpose of Pub.L. 100-238, see 1988 U.S. Code Cong. and Adm. News, p. 3217.

SUBPART H—ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

CHAPTER 91—ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Sec.

9101. Criminal history record information for national security purposes.

§ 9101. Criminal history record information for national security purposes

(a) As used in this section:

(1) The term "criminal justice agency" includes Federal, State, and local agencies and means: (A) courts, or (B) a Government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or Executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(2) The term "criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. The term does not include

those records of a State or locality sealed pursuant to law from access by State and local criminal justice agencies of that State or locality.

(3) The term "classified information" means information or material designated pursuant to the provisions of a statute or Executive order as requiring protection against unauthorized disclosure for reasons of national security.

(4) The term "State" means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, the Virgin Islands, American Samoa, the Trust Territory of the Pacific Islands, and any other territory or possession of the United States.

(5) The term "local" and "locality" means any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal, or other local government level.

(b)(1) Upon request by the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency or the Federal Bureau of Investigation, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by such department, office, agency or bureau for the purpose of determining eligibility for (A) access to classified information or (B) assignment to or retention in sensitive national security duties. Such a request to a State central criminal history record repository shall be accompanied by the fingerprints of the individual who is the subject of the request if required by State law and if the repository uses the fingerprints in an automated fingerprint identification system. Fees, if any, charged for providing criminal history record information pursuant to this subsection shall not exceed the reasonable cost of providing such information, nor shall they in any event exceed those charged to State or local agencies other than criminal justice agencies for such information.

(2) This subsection shall apply notwithstanding any other provision of law or regulation of any State or of any locality within a State, or any other law of the United States.

(3)(A) Upon request by a State or locality, the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency, or the Federal Bureau of Investigation shall enter into an agreement with such State or locality to indemnify and hold harmless such State or locality, and its officers, employees and agents, from any claim against such State or locality, or its officer, employee or agent, for damages, costs and other monetary loss, whether or not suit is instituted, arising from the disclosure or use by such department, office, agency or bureau of criminal history record information obtained from the State or locality pursuant to this subsection, if the laws of such State or locality, as of the date of enactment of this section, otherwise have the effect of prohibiting the disclosure of such criminal history record information to such department, office, agency or bureau.

(B) When the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency or the Federal Bureau of Investigation and a State or locality have entered into an agreement described in subparagraph (A), and a claim described in such subparagraph is made against such State or locality, or its officer, employee, or agent, the State or locality shall expeditiously transmit notice of such claim to the Attorney General and to the United States Attorney of the district embracing the place wherein the claim is made, and the United States shall have the opportunity to make all determinations regarding the settlement or defense of such claim.

(c) The Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency, or the Federal Bureau of Investigation shall not obtain criminal history record information pursuant to this section unless it has received written consent from the individual under investigation for the release of such information for the purposes set forth in paragraph (b)(1).

(d) Criminal history record information received under this section shall be disclosed or used only for the purposes set forth in paragraph (b)(1) or for national security or criminal justice purposes authorized by law, and such information shall be made available to the individual who is the subject of such information upon request.

(e) The authority provided under this section with respect to the Department of State may be exercised only so long as the Department of State continues to extend to its employees and applicants for employment, at a minimum, those procedural safeguards provided for as part of the security clearance process that were made available, as of May 1, 1987, pursuant to section 163.4 of volume 3 of the Foreign Affairs Manual.

(Added Pub.L. 99-169, Title VIII, § 801(a), Dec. 4, 1985, 99 Stat. 1008, and amended by Pub.L. 99-549, Title IV, § 402(a), Oct. 27, 1986, 100 Stat. 3196; Pub.L. 101-246, Title I, § 114, Feb. 16, 1990, 104 Stat. 22.)

Historical and Statutory Notes

1990 Amendment. Subsec. (b)(1). Pub.L. 101-246, § 114(1), inserted "the Department of State," after "Defense."

Subsec. (b)(3). Pub.L. 101-246, § 114(1), inserted "the Department of State," after "Defense," wherever appearing.

Subsec. (c). Pub.L. 101-246, § 114(1) inserted "the Department of State," after "Defense."

Subsec. (e). Pub.L. 101-246, § 114(2), added subsec. (e).

1986 Amendment. Subsec. (b)(1). Pub.L. 99-549, § 402(a)(1), added reference to the Federal Bureau of Investigation and reference to such bureau.

Subsec. (b)(3)(A). Pub.L. 99-549, § 402(a)(2), added reference to the Federal Bureau of Investigation and reference to such bureau wherever appearing.

Subsec. (b)(3)(B). Pub.L. 99-549, § 402(a)(3), added reference to the Federal Bureau of Investigation.

Subsec. (c). Pub.L. 99-549, § 402(a)(4), added reference to the Federal Bureau of Investigation.

Effective Date of 1986 Amendment. Section 402(c) of Pub.L. 99-549 provided that: "The amendments made by this section [amending this section and section 803(a) of Pub.L. 99-169 set out as a note under this section] shall become effective with respect to any inquiry which begins after the date of enactment of this Act [Oct. 27, 1986] conducted by the Federal Bureau of Investigation for purposes specified in paragraph (b)(1) of section 9101 of title 5, United States Code [subsec. (b)(1) of this section]."

Effective Date. Section 802 of Pub.L. 99-169 provided that: "The amendments made by section 801(a) of this Act [amending this section], shall become effective with respect to any inquiry which begins after the date of enactment of this Act [Dec. 4, 1985], conducted by the Department of Defense, the Office of Personnel Management, or the Central Intelligence Agency, for the purposes specified in paragraph (b)(1) of section 9101

of title 5, United States Code, as added by this Act [subsec. (b)(1) of this section]."

Extension of Termination Date of Subsection (b)(3) of this Section. Pub.L. 100-453, Title I, § 101(d), Sept. 29, 1988, 102 Stat. 1904, provided that: "The expiration date provided for in section 803(b) of the Intelligence Authorization Act for Fiscal Year 1986 (Public Law 99-107) [set out as a note under this section] shall be extended until December 31, 1989."

Report to Congressional Committees on Effect of Provisions for Indemnification Agreements. Section 803(a) of Pub.L. 99-169 as amended by Pub.L. 99-549, Title IV, § 402(b), Oct. 27, 1986, 100 Stat. 3196 provided that: "Within two years after the date of enactment of this Act [Dec. 4, 1985], the Department of Justice, after consultation with the Department of Defense, the Office of Personnel Management, the Central Intelligence Agency, and the Federal Bureau of Investigation, shall report to the appropriate committees of the Congress concerning the effect of section 9101(b)(3) of title 5, United States Code, as added by this Act [subsec. (b)(3) of this section], including the effect of the absence of indemnification agreements upon States and localities not eligible under section 9101(b)(3) of title 5, United States Code, for such agreements."

Termination Date of Subsection (b)(3) of This Section. Section 803(b) of Pub.L. 99-169 provided that: "(b) Three years after the date of enactment of this Act [Dec. 4, 1985], section 9101(b)(3) of title 5, United States Code [subsec. (b)(3) of this section], shall expire."

Legislative History. For legislative history and purpose of Pub.L. 99-169, see 1985 U.S. Code Cong. and Adm. News, p. 932. See, also, Pub.L. 99-549, 1986 U.S. Code Cong. and Adm. News, p. 5327; Pub.L. 101-246, 1990 U.S. Code Cong. and Adm. News, p. 3.

Library References

Records 460.

C.J.S. Records § 36.

DRAFT

MEMORANDUM OF AGREEMENT

CRIMINAL JUSTICE INFORMATION SYSTEMS

WHEREAS, the City of _____ Information System Department operates an electronic data processing and computer center to store and process certain criminal justice information; and

WHEREAS, the City of _____ is desirous of interfacing its computer system with the _____ Criminal Justice Information System _____ and

WHEREAS, it is a prerequisite for accessing _____ via computer interface that the concerned computer operations be under the management of a criminal justice agency; and

WHEREAS, it is not the purpose of this agreement to intringe upon or impair the normal right of the manager of the _____ Information System Department to make and place in effect his decisions concerning the operation of the Information Systems Department (ISD), any of the rights, powers, or authority the Information Systems Manager had prior to the signing of this agreement is retained, except that specifically abridged, delegated, granted, or modified by this agreement; and

WHEREAS, various statutes, regulations and rules require that certain conditions be met to ensure the privacy and security of criminal justice information in local computer systems; and

WHEREAS, this resolution is necessary to comply with those requirements, and to obtain authorization for the City of _____ to interface its computer with that of the _____ Department of Public Safety;

DRAFT

IT IS, THEREFORE, AGREED AS FOLLOWS:

A. The Chief of the Police Department is hereby designated to have management control of the Information Systems Department computer operations insofar as they are utilized in the storage, processing, handling, and dissemination of criminal justice information, and the Chief, or his representative, is authorized to take all action necessary to put and keep the Data Processing Department in compliance with all statutes, regulations and other laws relating to the privacy and security of computerized criminal justice information. Management Control shall include, but not be limited to, the right to do the following things:

1. Set and enforce priorities and policies governing the operation of computers, circuits, and telecommunications terminals to process criminal justice information, insofar as that equipment is used to process, store or transmit criminal justice information;
2. Set and enforce standards for the selection, supervision and termination of personnel involved in the processing, storing or transmitting of criminal justice information;
 - a. The Information System Department agrees the Police Department will screen and have the right to reject for employment or assignment any personnel proposed to be authorized for access to the criminal justice information systems.

BEST COPY AVAILABLE

DRAFT

- b. The Information System Department agrees to initiate, or permit the Police Department to initiate, administrative action leading to the immediate transfer or removal of Information Systems Department employees where such employees are believed to have violated provisions of Title 23, Code of Federal Regulations, or the provisions of the Criminal Justice Information System User Agreement with the Department of Public Safety, or other security requirements established for the collection, storage, or dissemination of criminal justice information.
 - c. The Police Department agrees the day-to-day supervision of employees of the Information Systems Department shall be the responsibility of the Information Systems Administrator.
3. The Information System Department and the Police Department agree that the Chief of the Police Department, or his representative, and the Department of Public Safety shall have the authority to independently or jointly inspect, monitor, and audit all procedures and systems pursuant to this agreement and any other matters concerned with the security of criminal justice information systems.

DRAFT

IN WITNESS WHEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

POLICE DEPARTMENT

REVIEW BY:

NCIC POLICIES FOR ACCESS AND DISSEMINATION OF III

1. "DUE TO VARIANCE IN STATE LAWS AND POLICIES, THE III CANNOT BE USED FOR LICENSING OR NONCRIMINAL JUSTICE EMPLOYMENT PURPOSES." (NCIC OM, 10-25, PARA 3.1) (11-1-87)
2. "THE III SHALL NOT BE USED FOR REMOTELY ACCESSING A RECORD TO BE REVIEWED AND/OR CHALLENGED BY THE SUBJECT OF THE RECORD. RECORD REQUESTS FOR THIS PURPOSE MUST BE SUBMITTED IN WRITING EITHER TO THE FBI IDENTIFICATION DIVISION OR STATE OF RECORD." (III OTM, INTRO-6) (7-1-91)
3. "COPIES OF CRIMINAL HISTORY DATA OBTAINED FROM TERMINAL DEVICES MUST BE AFFORDED SECURITY TO PREVENT ANY UNAUTHORIZED ACCESS TO OR USE OF THAT DATA." (NCIC OM, 10-20, PARA VII (C-3) (11-17-86)
4. "EACH CRIMINAL JUSTICE AGENCY RECEIVING AN III RESPONSE SHALL RECORD ANY SECONDARY DISSEMINATION OF ANY III RESPONSE TO ANOTHER CRIMINAL JUSTICE AGENCY OR AN INDIVIDUAL WITHIN ANOTHER AGENCY, OR TO ANYONE LEGALLY ENTITLED TO RECEIVE SUCH INFORMATION WHO IS OUTSIDE THE ORIGINAL RECEIVING AGENCY. THESE LOGS SHALL BE MAINTAINED FOR AT LEAST 12 MONTHS. (ADVISORY POLICY BOARD MINUTES, PAGE 310) (10-84)
5. "AUDIO RESPONSE TERMINALS AND RADIO DEVICES, WHETHER DIGITAL OR VOICE, SHALL NOT BE USED ROUTINELY FOR THE TRANSMISSION OF CRIMINAL HISTORY BEYOND THAT INFORMATION NECESSARY TO EFFECT AN IMMEDIATE IDENTIFICATION OR TO ENSURE ADEQUATE SAFETY FOR OFFICERS AND THE GENERAL PUBLIC. WHEN AN OFFICER DETERMINES THERE IS AN IMMEDIATE NEED FOR THIS INFORMATION TO FURTHER AN INVESTIGATION OR THERE IS A SITUATION AFFECTING THE SAFETY OF AN OFFICER OR THE GENERAL PUBLIC, THEN DETAILS OF CRIMINAL HISTORY MAY BE TRANSMITTED. (NCIC OM, 10-20, PARA VII (B-3)

- NCIC AUDIT STAFF -
SECURITY COMPLIANCE CHECKLIST

PERSONNEL SECURITY:

YES

NO

1. How is physical access to terminal sites controlled? _____
2. Does the agency screen employees having access to the terminal/NCIC information? _____
3. How are the employees accessing NCIC information screened? _____

TECHNICAL SECURITY:

1. Does the agency utilize passwords to access the terminals? _____
2. How are the passwords controlled by the agency? _____
3. Are mobile terminals utilized by the agency? If yes, test access. _____
4. Do the mobile terminals have:
Entry capabilities? _____
III capabilities? _____
Inquiry only capabilities? _____
5. How is access controlled for mobile terminals? Explain. _____
6. If mobile terminals access III, describe the security precautions in effect at the agency. _____

The Washington Post

18 Charged With Lifting U.S. Computer Data

Associated Press

NEWARK, N.J., Dec. 18—Eighteen private investigators or Social Security Administration employees in nine states were charged today with buying and selling confidential data from federal government computers.

The investigators paid for personal information illegally pinched from the SSA and the Federal Bureau of Investigation, U.S. Attorney Michael Chertoff said.

The confidential data—personal earnings histories and criminal records—were not taken by outside hackers breaking into the system, Chertoff said, but by government employees exploiting their access to the system.

The private eyes either bribed or

duped government workers to provide the confidential information, Chertoff said.

The private investigators, many of whom advertise in legal journals, sold the information to private companies, Chertoff said. Companies could use the information to track people down or make decisions on hiring, firing, suing or lending.

Prosecutors in New Jersey and Tampa filed the charges in their home states because they started the investigation.

The earnings information was allegedly pinched from the SSA computer system, which houses earnings and employment information on all people with social security numbers. The criminal histories were allegedly taken from the

EBL's, National Crime Information Center, which provides criminal information to federal, state and local law enforcement agencies throughout the country.

If convicted on all counts against them, the defendants face maximum sentences of 20 to 150 years and multimillion-dollar fines.

Named in both the New Jersey and Florida indictments were Linda Stollenwerck, who works in the SSA's Melrose Park, Ill., office, and George Theodoreakopolous, who owns Tracers Worldwide Services of Corpus Christi, Tex., and Elmhurst, Ill.

Indicted in New Jersey were Allen and Petra Schweitzer, a married couple who own the Security Group in Sumner, Wash.; Edward Fleming,

owner of Super Bureau in Monterey, Calif., and his daughter, Susan Fleming; Victor Fought, operator of Locate Unlimited in Mesa, Ariz.; Richard Stone, owner of Interstate Information Services in Port Jefferson, N.Y., and Michael Hawes, former owner of International Criminal Investigative Agency in Port Angeles, Wash.

Indicted in Florida were Robert Boland, an employee of the Fulton County Sheriff's office in Georgia; Gail Mullinax, a private investigator in Austell, Ga.; William Pedersen, a Chicago police officer; Jack Hauser, an investigator from Grand Rapids, Mich.; Ronald Cianciosi, an investigator from Coral Springs, Fla.; John Colesanti, a SSA employee in New York City; Robert Bressette of Phoenix; Joanna Price, a former SSA employee in Phoenix, and Frank Farrington of Seattle.

Theft of U.S. Data Seen as

Growing Threat to Privacy

By Michael Isikoff
Washington Post Staff Writer

Need somebody checked out? Just call "Nationwide Electronic Tracking," or NET, the company that "Gets the Information You Need—When You Need It."

So boasted a sales brochure sent out last year by the Tampa firm claiming "instant access" to a wide range of "confidential" computer data. For fees ranging from \$5 to \$175, NET promised, it could provide customers with data on virtually anyone in the country—private credit reports, business histories, driver's license records, even personal Social Security records and criminal history backgrounds.

NET may have seemed like a boon to companies trying to check applicants or even homesuspicious of their new neighbors across the street. But some federal officials say it also was evidence of a growing computer-age menace—the fledgling "information broker" industry that some experts fear may pose one of the most serious threats to individual privacy in decades.

Law enforcement officials say that as the demand for personal data grows, information brokers are increasingly turning to illegal methods. Last week, NET was identified by the FBI as one player in a nationwide network of brokers and private investigators who allegedly were pilfering confidential personal data from U.S. government computers and then selling them for a fee to lawyers, insurance companies, private employers and other customers.

The information-broker investigation involved what officials say was the largest case ever involving the theft of federal computer data and was all the more striking because it was essentially a series of jobs. Among the 16 people

arrested by the FBI in 10 states were three current or former Social Security Administration employees (in Illinois, New York and Arizona) charged with selling personal records contained in SSA computers.

Those records, retained for about 200 million Americans, include a person's Social Security number, full name, place of birth, date of birth, names of both parents, names of all current and past employers, and the person's salary—year by year—since he or she began working, said Philip Gambino, chief spokesman for the SSA.

Also arrested was a Chicago police officer and a terminal operator at the Fulton County, Ga., sheriff's office. Both were charged with illegally retrieving criminal history records from the FBI's National Criminal Information Center (NCIC), another highly sensitive database that contains records of about 15,170,000 arrests compiled from local law enforcement agencies around the country.

About 62,000 police and criminal justice agencies have access to the system, and "within each agency there may be dozens of authorized users," said a congressional staff member who has studied the problem. "So it's very hard to identify anomalous or improper transactions."

In effect, law enforcement officials said, information brokers like NET were bribing the government employees to run computer checks on individuals for as little as \$50 a pop. Computer checks were being run "on thousands of people," said Jim Cottos, regional inspector general in Atlanta for the Department of Health and Human Services, whose office launched the investigation.

"This was not a once-a-week activity," said Cottos. "These guys [the information brokers] were making big bucks. We're talking about a couple of hundred thousands dollars a year."

To many experts, the case suggests that "insider" information trading may be far more widespread than previously suspected. For the past several years, while the news media have focused on the threat posed by outside computer hackers, law enforcement officials have been making a growing number of cases against computer "insiders" who sell data to private companies.

Last May, for example, a Virginia State Police officer was indicted on charges of selling NCIC records to two Prince George's County private investigators, who allegedly charged clients \$200 for each criminal record check. In other recent cases, public employees have been charged with illegally selling—and in some cases, altering—driver's license records, Social Security records and a wide variety of other government data supposedly protected by privacy laws.

"The public is abysmally uninformed about problems like this," said Peter Neumann, a computer security expert and principal scientist at the computer science laboratory at SRI International, a Menlo Park, Calif., think tank. "With sufficient access to a few databases these days, you can get pretty close to somebody's life history with nothing more than a Social Security number."

Private info sold by ring, FBI says

By Jerry Seper
THE WASHINGTON TIMES

The FBI arrested 18 persons in 10 states yesterday on conspiracy and bribery charges stemming from the sale of confidential income tax, arrest and work history information on hundreds of people.

The confidential information, housed in government computers, was sold to insurance companies, lawyers and private investigators, the FBI said.

The arrests culminated an 18-month investigation by the FBI and the Department of Health and Human Services.

The charges came in 10 separate federal grand jury indictments returned earlier this month and unsealed yesterday in Newark, N.J., and Tampa, Fla.

"Every person in this country has the right to expect that personal information will only be released for legitimate purposes," FBI Director William S. Sessions said.

"The FBI is deeply concerned about the integrity of this information and will continue to vigorously investigate any individuals who compromise the public's right to privacy," he said.

The indictments allege the information included computer data on arrest records from the National Crime Information Network, housed at the FBI; income tax, earnings and employment histories from the Social Security Administration (SSA); telephone company records; and "other protected government information concerning private citizens."

The defendants — named on charges of bribery, conspiracy, theft of government property and unauthorized disclosure of income tax information — face prison terms ranging from 20 to 150 years and fines as high as \$3.25 million.

The indictments say the defendants obtained private information from FBI and SSA computers by bribing "government employees who had access to the information."

The government employees were identified as Linda Stollenwerck, a claims development clerk at the SSA in Melrose Park, Ill.; Joanna C. Price, a former SSA employee in Phoenix; John Colesanti, a SSA employee in New York City; William L. Pedersen, a Chicago police officer; and Robert M. Boland, a computer operator at the Fulton County Sheriff's Department in Atlanta.

Mr. Pedersen also is named in a separate indictment on charges of conspiracy to defraud the FBI, the sale of government records, wire fraud and making false statements to federal investigators. He faces 50 years in prison and fines totaling \$1.75 million.

Others arrested, according to the indictments, were described as "information brokers" in New York, California, Arizona, Texas, Washington, Idaho, New Jersey, Michigan, Florida and Georgia.

The indictments said the defendants conspired to pay the government employees for the information and then to sell it to potential buyers. None of the insurance companies, lawyers or private investigators was identified or indicted. The conspiracy, according to the indictment, began in December 1988 and continued through July 1991.

"Confidential government files and a U.S. citizen's right to privacy should not be sold to the highest bidder," said U.S. Attorney Michael Chertoff in Newark. He added that the investigation was continuing, but he declined to elaborate.

FBI spokesman Larry Curtain in Tampa said some of the information brokers advertised the sale of the computer data in local newspapers. He said one of the defendants referred to himself in a recent newspaper story as the "prince of information."

"He's probably thinking right now that someone has turned him back into a frog," Mr. Curtain said.

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: NCIC STANDARDS AND SANCTIONS

TITLE OF INSTRUCTION: NCIC Standards and Sanctions
TIME ALLOTTED: 1 Hour
TARGET GROUP: Full Access Terminal Operators
INSTRUCTOR:
METHOD OF INSTRUCTION: Lecture, Discussion, and
Overhead Transparencies
DATE: July 1, 1992

7/1/92

SAS-11

PREFACE

The NCIC Standards and Sanctions lesson plan is divided into seven parts. Below is an explanation of each part. Please review this section prior to instruction.

I. INTRODUCTION

This is a brief statement that is intended to obtain the interest of the trainee.

II. POLICY

This section defines policy for NCIC purposes and briefly describes the function of the administrative body that is responsible for recommending and approving NCIC policy.

III. AUDIT PROGRAM

This section describes the development of the audit program, the audit mandate as approved by the NCIC Advisory Policy Board, and the Federal and state responsibilities for instituting an audit program.

IV. TRAINING PROGRAM

This section describes the development of the training program, the NCIC training policy as approved by the NCIC Advisory Policy Board, and the Federal and state responsibilities for instituting a training program.

V. STANDARDS

This section defines a standard for NCIC purposes and describes the standards that must be followed in order for NCIC to be an effective communications network.

VI. SANCTIONS

This section defines a sanction for NCIC purposes. The two ultimate sanctions available to NCIC management for the enforcement of System policy and procedure, reasons why sanctions can be imposed for failure to comply, and the sanction process is also discussed.

VII. CONCLUSION

This section highlights the important points to remember that are associated with NCIC Standards and Sanctions.

NCIC STANDARDS AND SANCTIONS LESSON PLAN
TABLE OF CONTENTS

	PAGE
STATEMENT OF GOAL AND OBJECTIVES	SAS-1
CRITERION TEST	SAS-2
CRITERION TEST ANSWERS	SAS-4
ITEMS AND MATERIALS	SAS-7
INTRODUCTION	SAS-8
POLICY	SAS-10
Definition of a Policy for NCIC Purposes	SAS-10
NCIC Advisory Policy Board	SAS-10
AUDIT PROGRAM	SAS-11
Background	SAS-11
Audit Mandate	SAS-11
Federal Responsibilities	SAS-11
State Responsibilities	SAS-12
TRAINING PROGRAM	SAS-13
Background	SAS-13
Training Policy	SAS-13
Federal Responsibilities	SAS-14
State Responsibilities	SAS-14
STANDARDS	SAS-15
Definition of a Standard for NCIC Purposes	SAS-15
NCIC Standards	SAS-15
SANCTIONS	SAS-22
Definition of a Sanction for NCIC Purposes	SAS-22
NCIC Sanctions	SAS-22
NCIC Management Sanction Process	SAS-23
CONCLUSION	SAS-26
BIBLIOGRAPHY	SAS-27

STATEMENT OF GOAL AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator with important information on NCIC standards, policies, and sanctions as approved by the NCIC Advisory Policy Board.

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the terminal operator will be able to:

1. Define a policy for NCIC purposes.
2. Describe the audit mandate as approved by the NCIC Advisory Policy Board.
3. Describe the two elements of the NCIC training policy that pertain to terminal operators.
4. Define a standard for NCIC purposes.
5. List three standards that must be followed by the local agency in order for NCIC to be an effective communications network.
6. Define a sanction for NCIC purposes.
7. Identify the two ultimate sanctions available to NCIC management (FBI NCIC and the Advisory Policy Board) for the enforcement of System policy and procedure.
8. List five reasons why sanctions could be imposed for failure to comply.
9. Describe the sanction process that is followed by NCIC management when it is determined that an agency has failed to comply with policy and procedure.

CRITERION TEST

POLICY SECTION

1. In accordance with lecture, define a policy for NCIC purposes.
2. From the following list, select the best answer that describes the function of the NCIC Advisory Policy Board:
 - a. Comprised of 30 members
 - b. Meet at least twice a year
 - c. Recommends general policy concerning the philosophy, concept, and operational principles of NCIC to the Director of the FBI.
 - d. All of the above

AUDIT SECTION

1. Describe the audit mandate as approved by the NCIC Advisory Policy Board.
2. Each CTA/FSC shall be audited by _____ at least once every _____ years.
3. All CTAs and FSCs shall institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of information in the system.
 - a. True
 - b. False

TRAINING SECTION

1. Since the inception of NCIC, training has been the primary responsibility of the individual _____.
2. Describe the two elements of the NCIC training policy that pertain to terminal operators.
3. A _____ is responsible for ensuring compliance with state and NCIC policy and regulations including validation requirements within their agency.

STANDARDS SECTION

1. In accordance with lecture, define a standard for NCIC purposes.
2. Availability for hit confirmation 24 hours a day is a standard that has been established and must be followed.
 - a. True
 - b. False
3. List three standards that must be followed by the local agency in order for NCIC to be an effective communications network.
 - a. _____
 - b. _____
 - c. _____

SANCTIONS SECTION

1. In accordance with lecture, define a sanction for NCIC purposes.
2. What are the two ultimate sanctions available to NCIC management for enforcement of policy and procedure?
3. List five reasons why sanctions could be imposed for failure to comply.
 - a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____
4. Briefly describe the sanction process that is followed by NCIC management when it is determined that an agency has failed to comply with policy and procedure.

CRITERION TEST ANSWERS

POLICY SECTION

1. For NCIC purposes, a policy is defined as a plan or course of action designed to influence and determine decisions and actions.
2. The NCIC Advisory Policy Board c. recommends general policy concerning the philosophy, concept, and operational principles of NCIC to the Director of the FBI.

AUDIT SECTION

1. The Advisory Policy Board stated that by December 31, 1986, each CTA and FSC shall establish a system to biennially audit every terminal agency to ensure compliance with state and NCIC policy and regulations.
2. Each CTA/FSC shall be audited by FBI NCIC at least once every two years.
3. a. True All CTAs and FSCs shall institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of information in the system.

TRAINING SECTION

1. Since the inception of NCIC, training has been the primary responsibility of the individual states.
2. The two elements of the NCIC training policy that pertain to terminal operators are:
 - a. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.
 - b. Biennially provide functional retesting, and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.
3. A Terminal Agency Coordinator is responsible for ensuring compliance with state and NCIC policy and regulations including validation requirements within their agency.

STANDARDS SECTION

1. For NCIC purposes, a standard is defined as the minimum level of acceptable performance that must be demonstrated and can be observed or measured.
2. a. True. Availability for hit confirmation 24 hours a day is a standard that has been established and must be followed.
3. Three standards that must be followed by the local agency in order for NCIC to be an effective communications network are:
 - a. Standards for Record Entry by User Agency
 - b. Standards for Agencies Receiving a Positive Response (Hit)
 - c. Standards Regarding Equipment and Technology Compatibility

SANCTIONS SECTION

1. For NCIC purposes, a sanction is defined as a penalty, specified or in the form of moral pressure, that acts to ensure compliance or conformity.
2. The two ultimate sanctions available to NCIC management for enforcement of policy and procedure: 1) purge of an agency's records and 2) discontinuance of system access.
3. Reasons why sanctions could be imposed for failure to comply are:
 - a. Failure to react properly to hit confirmation requests
 - b. Failure to locate
 - c. Failure to complete entries/modifications/removals promptly
 - d. Failure to make complete entries
 - e. Failure to validate
 - f. Failure to assure security of equipment and data
 - g. Failure to provide trained operators
 - h. Entry of invalid or inaccurate records
 - i. Failure to meet requirements for training users of the System
 - j. Failure to meet requirements to biennially audit every terminal agency

4. The sanction process that is followed by NCIC management when it is determined that an agency has failed to comply with policy and procedure is:
- a. An audit of the CTA is conducted and the results are presented to the Sanctions Ad Hoc Subcommittee during the NCIC Advisory Policy Board meeting.
 - b. The Subcommittee reviews the audit for compliance with NCIC policy, quality of information placed in the system, and the level of NCIC access provided to local users by the servicing state or Federal agency.
 - c. A letter of request for compliance is sent to the CTA who will send a letter to the offending terminal agency.
 - d. A letter of intent to remove from the system or an advisory letter to the governor may be sent.
 - e. If necessary, sanctions are enforced pending reinstatement of the CTA/state and/or the offending agency.
 - f. Upon satisfactory proof of correction of its deficiencies, the Board may reinstate the CTA and the CTA may reinstate the offending terminal.

ITEMS AND MATERIALS:

Overhead Transparencies, Overhead Projector, and Screen,
VCR, and Monitor

Video Tape: "NCIC System Security"

OVERHEAD TRANSPARENCIES (OH):

SAS-OH #1 NCIC Standards and Sanctions
SAS-OH #2 Definition of a Policy for NCIC Purposes
SAS-OH #3 NCIC Advisory Policy Board
SAS-OH #4 Audit Mandate
SAS-OH #5 NCIC Training Policy
SAS-OH #6 Terminal Agency Coordinator (TAC) Responsibilities
SAS-OH #7 Definition of a Standard for NCIC Purposes
SAS-OH #7a Definition of a Standard for NCIC Purposes (Cont).
SAS-OH #8 NCIC Standards
SAS-OH #9 Introduction Section 5 -- NCIC Standards and
Sanctions (NCIC Inquiries Hot Files/III and NCIC
Record Entry)
SAS-OH #10 Standards for System Availability--Computer
Availability Goals
SAS-OH #11 Definition of a Sanction for NCIC Purposes
SAS-OH #12 Two Ultimate Sanctions Available to NCIC Management
SAS-OH #13 Reasons Why Sanctions Could Be Imposed

HANDOUT MATERIALS (HD):

SAS-HD #1 "Loss of FBI Computer Leaves a Void in Bamberg
County Law Enforcement"
SAS-HD #2 "Bamberg To Employ Dispatcher"
SAS-HD #3 Audit Plan
SAS-HD #4 Letter to all CTOs and FSCs - Reformulation of
NCIC Training Policy
SAS-HD #5 Introduction Section 5 -- NCIC Standards and
Sanctions (NCIC Inquiries Hot Files/III and NCIC
Record Entry)
SAS-HD #6 Current NCIC System
SAS-HD #7 National Crime Information Center User Agreement

I. INTRODUCTION

THIS ONE-HOUR BLOCK OF INSTRUCTION IS DESIGNED TO INFORM THE TERMINAL OPERATOR OF NCIC STANDARDS, POLICIES, AND SANCTIONS AS APPROVED BY THE NCIC ADVISORY POLICY BOARD.

THE INSTRUCTOR SHOULD WELCOME AND INTRODUCE SELF TO THE GROUP; EXPLAIN COURSE GOAL AND OBJECTIVES; REVIEW AND DISTRIBUTE HANDOUT MATERIALS.

The National Crime Information Center is a vast communications network that was established to serve all criminal justice agencies on a local, state, and Federal level. The National Crime Information Center (NCIC) became operational on January 27, 1967.

NCIC makes centralized criminal justice data immediately available. The goal of NCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of timely and accurate documented criminal justice information. Policies, procedures, and standards have been set forth and must be strictly adhered to in order for the system to produce the expected results. But, what happens when they are not followed?

The following is an account of what happened to one agency that failed to provide 24-hour coverage for their terminal.

References

IO - Instructional Objective

OH - Overhead Transparency

HD - Handout Material

OH #1

HD #1,2

The agency did not provide around-the-clock, seven-day-a-week teletype monitoring by a dispatcher. NCIC policy states, "agencies that enter records into NCIC must ensure that hit confirmation is available 24 hours a day either at that agency or through another agency, providing a written agreement has been executed." When policies and standards are not complied with, there are sanctions available to NCIC management that may be enforced. The state CTA advised the agency that they could no longer enter information into NCIC because of their failure to meet state and Federal guidelines. However, use of the computer could be regained once it was in compliance. The agency temporarily lost a valuable tool.

The information presented in this lesson plan will enhance the knowledge of the terminal operator regarding important information on NCIC standards, policies, and sanctions as approved by the NCIC Advisory Policy Board.

II. POLICY

A. Definition of a Policy for NCIC Purposes

1. A policy is defined as a plan or course of action designed to influence and determine decisions and actions.

IO #1

OH #2

B. NCIC Advisory Policy Board

1. The NCIC Advisory Policy Board*, comprised of 30 representatives from criminal justice agencies throughout the United States, is responsible for recommending general policy to the FBI with respect to the philosophy, concept, and operational principles of the NCIC.

OH #3

***INSTRUCTOR'S NOTE: REFER TO THE SHARED MANAGEMENT CONCEPT LESSON PLAN FOR FURTHER INFORMATION ON THE NCIC ADVISORY POLICY BOARD.**

2. Critical policies that have been established by the Board include, but are not limited to:

- Validation Requirements†
- Hit Confirmations†
- III Logging Requirements†
- Audit Requirements
- Training Policy
- Terminal Agency Coordinator (TAC) Definition
- Second Party Checks‡

†INSTRUCTOR'S NOTE: REFER TO THE NCIC VALIDATION, HIT CONFIRMATION, AND INTERSTATE IDENTIFICATION INDEX LESSON PLANS FOR FURTHER INFORMATION.

‡REFER TO THE ENTRY SECTION, POLICY ISSUES PART OF EACH NCIC "HOT" FILE LESSON PLAN.

III. AUDIT PROGRAM

A. Background

1. At the December, 1982, APB meeting, the recommendation was made by the Quality Assurance Subcommittee to the Board for NCIC to formalize an objective audit program for CTAs and other agencies with direct lines to NCIC to ensure continuing high quality NCIC service.
 - a. This program must include guidelines that could be used by the CTA to perform similar audits of local users of NCIC services, consistent with policy already established for NCIC use.
2. The NCIC Audit Program was implemented in 1983 with the goal of assessing policy compliance and data quality within each state.

B. Audit Mandate

1. The Advisory Policy Board stated that by December 31, 1986, each CTA and FSC shall establish a system to biennially audit every terminal agency to ensure compliance with state and NCIC policy and regulations.

C. Federal Responsibilities

1. Each CTA/FSC shall be audited by FBI NCIC at least once every two years (biennially).
2. The audit examines five basic areas:
 - a. General administrative management of the system, including training
 - b. Security, including personnel and technical matters
 - c. Quality assurance, including state audit mechanisms

IO #2
OH #4

HD #3
PP. vi-vii

d. System performance

e. Data quality assessment

3. The audit includes reviewing data quality and assessing compliance with critical policy at a sample of state and local criminal justice agencies.

D. State Responsibilities

1. All CTAs and FSCs shall institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of information in the system.

IV. TRAINING PROGRAM

A. Background

1. Since the inception of NCIC, training has been the primary responsibility of the individual states.
2. During 1983 and 1984, audits by the NCIC Audit Staff found great variability in both the type and quality of training provided to users.
3. Without proper training on the use of NCIC and state computer systems, agencies accessing NCIC cannot ensure that employees are following policy and procedure and performing their duties as efficiently and accurately as possible.
4. In October, 1984, in response to the findings of the NCIC Audit Staff, the Advisory Policy Board established a mandatory training program.

B. Training Policy

1. The Advisory Policy Board stated that by December 31, 1986, each CTA shall establish a system which will include, but is not limited to*:
 - a. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.
 - b. Biennially provide functional retesting and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

***INSTRUCTOR'S NOTE: 1. A. AND B. REFER SPECIFICALLY TO TERMINAL OPERATORS. PLEASE REFER TO THE HANDOUT FOR FURTHER INFORMATION CONCERNING THE TRAINING POLICY AS APPROVED BY THE APB (OCTOBER, 1984). THE**

IO #3
OH #5
HD #4

APB LATER APPROVED THE REFORMULATION OF THE NCIC TRAINING POLICY AND NCIC ADVISED ALL CTOS AND FSCS BY A MEMORANDUM DATED 9/11/91.

1. B. REFLECTS THE CHANGES MADE TO THE TRAINING POLICY.

CONTACT THE NCIC TRAINING STAFF AT (202) 324-6090 TO OBTAIN COPIES OF THE MANDATORY MINIMUM CURRICULUM LESSON PLANS FOR FULL ACCESS TERMINAL OPERATORS.

C. Federal Responsibilities

1. FBI NCIC responsibility under the shared management concept includes providing training and training materials to the control terminal agencies.

D. State Responsibilities

1. The CTO shall be responsible for providing adequate training to agencies accessing NCIC through the CTA computer.
2. Each CTO shall ensure that each terminal agency administrator designate an individual to function as a **Terminal Agency Coordinator (TAC)*** who shall be responsible for ensuring compliance with state and NCIC policy and regulations including validation requirements.

OH #6

***INSTRUCTOR'S NOTE: CHECK WITH YOUR STATE CTA OR FSC FOR FURTHER INFORMATION CONCERNING THE RESPONSIBILITIES OF TAC WITHIN YOUR STATE.**

V. STANDARDS

A. Definition of a Standard for NCIC Purposes

1. A standard is defined as the minimum level of acceptable performance that must be demonstrated and can be observed or measured.
2. Standards provide a tool of measurement against which the NCIC Advisory Policy Board can measure the performance of the component parts of the NCIC System as a whole.

IO #4

OH #7

OH #7a

B. NCIC Standards

1. In order for NCIC to be an effective communications network, standards must be established, adopted, and followed:

IO #5

OH #8

INSTRUCTOR'S NOTE: OH #8 LISTS EACH OF THE NCIC STANDARDS. INFORM STUDENTS THAT EACH WILL BE DISCUSSED SEPARATELY. EMPHASIZE THAT STANDARDS FOR RECORD ENTRY BY USER AGENCY, AGENCIES RECEIVING A POSITIVE RESPONSE (HIT), AND EQUIPMENT AND TECHNOLOGY COMPATIBILITY, APPLY TO THE LOCAL AGENCY. ALSO, HAVE STUDENTS REFER TO HD#5 IN PREPARATION FOR THE DISCUSSION ON STANDARDS FOR RESPONSE TIME.

a. Standards for Inquiry Response Time

OH #9

(1) Hot Files

HD #5

EXAMPLE A

(a) State CTA Computer

- 1) The average message response time for an inquiry from the

SCTA to NCIC and back to the SCTA should not exceed two seconds.

- 2) The average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 12 seconds after transmission of the inquiry (with two of the 12 seconds allotted to the transmission to, processing by, and return of the response from NCIC).

(b) Local/Regional Computer

HD #5
EXAMPLE A

- 1) The average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 22 seconds after transmission of the inquiry (with 12 of the 22 seconds allotted to the transmission to, processing by, and return of the response from the SCTA and NCIC).
- 2) The average response time from any local/regional system or terminal interfaced directly with the NCIC computer to an end user terminal interfaced with the local/regional system shall not exceed 12 seconds (with two of the 12 seconds allotted to the transmission to, processing by, and return of the response from NCIC).

(2) Interstate Identification Index

HD #5
EXAMPLE B

(a) SCTA Computer

- 1) The average message response time for an inquiry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.

- 2) The average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 15 seconds after transmission of the inquiry (with five of the 15 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC).

(b) Local/Regional Computer

HD #5
EXAMPLE B

- 1) The average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 25 seconds after transmission of the inquiry (with 15 of the 25 seconds allotted to the transmission to, processing by, and return of the response from the SCTA and NCIC).
- 2) The average response time from any local/regional system or terminal interfaced directly with the NCIC computer to an end user terminal interfaced with the local/regional system shall not exceed 15 seconds (with five of the 15 seconds allotted to the transmission to, processing by, and return of the response from NCIC).

INSTRUCTOR'S NOTES: THE TIMES INDICATED IN THE ABOVE STANDARDS ARE FOR HIGH-SPEED LINES ONLY. AN ADDITIONAL 10 SECONDS SHOULD BE ADDED TO THE ABOVE TIMES FOR EACH LOW-SPEED LINE INTERFACE, WITH FIVE SECONDS ALLOCATED TO THE INQUIRY AND FIVE SECONDS TO THE RESPONSE.

b. Standards for Record Entry by User Agency

- (1) Any agency having investigative authority and jurisdiction and having an NCIC ORI must enter records into NCIC which meet NCIC criteria as soon as reasonably possible after minimum information is available.*

***INSTRUCTOR'S NOTE: REEMPHASIZE THAT AGENCIES THAT ENTER RECORDS INTO NCIC ARE RESPONSIBLE FOR THEIR ACCURACY, TIMELINESS, AND COMPLETENESS. FOR FURTHER INFORMATION REGARDING RECORD ENTRY, SEE THE ENTRY SECTION OF EACH NCIC "HOT" FILE LESSON PLAN.**

- (2) Every agency which enters records into NCIC must assure that "hit" confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location.
- (3) Every agency is responsible for the removal of its NCIC record as soon as it is aware that the record is no longer valid.
- (4) The average message response time for an entry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.**

****INSTRUCTOR'S NOTE: REFER TO HD#5 FOR FURTHER INFORMATION ON STANDARDS FOR RECORD ENTRY INTO NCIC.**

c. Standards for Agencies Receiving a Positive Response (Hit)

- (1) Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any actions (i.e.,

arresting the wanted person,
detaining the missing person, or
seizing the stolen property) based
upon the hit NCIC record.

**INSTRUCTOR'S NOTE: REFER TO THE HIT CONFIRM-
ATION LESSON PLAN FOR FURTHER DETAILS ON THE
REQUIREMENTS FOR CONFIRMING AN NCIC HIT.**

d. Standards for System Availability

(1) System availability is based on
two factors*.

(a) The system is available when:

- 1) All services are available.
- 2) Inquiry only service is
available if the system
provides a response to the
inquiry (reasonable time
period).
- 3) One file is down for
scheduled file maintenance,
but other files are available
(reasonable time period).

(b) The system is down when:

- 1) No response is provided.
- 2) The entire mainframe is
down for maintenance,
either scheduled or
unscheduled.
- 3) Multiple files are unavail-
able for an extended
period.
- 4) Lines or circuits are down.

***INSTRUCTOR'S NOTE: THE ABOVE FACTORS ARE
USED BY THE NCIC AUDIT STAFF TO MEASURE
SYSTEM AVAILABILITY.**

(2) The computer availability goals are:

- (a) NCIC Computer - 100% with 99% as minimum acceptable performance
- (b) SCTA Computer - 100% with 96% as minimum acceptable performance
- (c) Local/Regional Computer - 100% with 96% as minimum acceptable performance

e. Standards Regarding Equipment and Technology Compatibility

- (1) Equipment and/or technological incompatibility shall not be sufficient justification for any agency to operate outside of the normal state CTA configuration.

f. Standards for Services Availability

- (1) Those services provided by NCIC to the state CTAs shall be provided by the state CTAs to their users with the exception of:
 - (a) Services specifically limited to SCTAs by NCIC policy.
 - (b) Services which are restricted to certain users by nature of their governmental and/or criminal justice status and Federal laws and regulations governing access to certain types of NCIC services.
 - (c) Services which may be contrary to a state law or executive order.

(2) Services include, but are not limited to:

- (a) Providing users with the capability of communicating with and receiving responses from all current and future NCIC Files.
- (b) The capability to enter an NCIC record into all current and future NCIC Files.
- (c) The capability to add information to, delete information from, and/or change information in a field(s) of an existing NCIC record.
- (d) The capability to remove a record from file when a record is determined to be invalid.
- (e) The capability to place a locate against another agency's NCIC record, including records entered by agencies serviced by same state CTA, as well as records entered by agencies serviced by another state CTA.

HD #6

INSTRUCTOR'S NOTE: USE OF THE ABOVE SERVICES BY ANY USER AGENCY SHALL BE IN ACCORDANCE WITH THE INSTRUCTIONS AND PROCEDURES CONTAINED IN THE NCIC OPERATING MANUAL, CODES CONTAINED IN THE NCIC CODE MANUAL, AND NEW ENHANCEMENTS CONTAINED IN THE NCIC TECHNICAL AND OPERATIONAL UPDATE, NCIC NEWSLETTER, OR ANY OTHER OFFICIAL NOTIFICATION FROM FBI NCIC.

VI. SANCTIONS

A. Definition of a Sanction for NCIC Purposes

1. A sanction is defined as a penalty, specified or in the form of moral pressure, that acts to ensure compliance or conformity.

IO #6

OH #11

B. NCIC Sanctions

1. There are two ultimate sanctions available to NCIC management (FBI NCIC and the Advisory Policy Board) for enforcement of policy and procedure:
 - a. Purge of an agency's records
 - b. Discontinuance of system access

IO #7

OH #12

INSTRUCTOR'S NOTE: CHECK WITH YOUR STATE CTA OR FSC TO IDENTIFY THE SANCTIONS WHICH MAY BE IMPOSED ON AGENCIES THAT FAIL TO COMPLY WITH NCIC/STATE POLICIES AND PROCEDURES.

2. The reasons why sanctions could be imposed for failure to comply include, but are not limited to:
 - a. Failure to react properly to hit confirmation requests
 - b. Failure to locate
 - c. Failure to complete entries/modifications/removals promptly
 - d. Failure to make complete entries
 - e. Failure to validate

IO #8

OH #13

- f. Failure to assure security of equipment and data
- g. Failure to provide trained operators
- h. Entry of invalid or inaccurate records
- i. Failure to meet requirements for training users of the System
- j. Failure to meet requirements to biennially audit every terminal agency

C. NCIC Management Sanction Process

IO #9

HD #7

- 1. An up-to-date NCIC/CTA user agreement, including reference to the sanctions that could be imposed for failure to comply, should be on file with NCIC and the CTA.
- 2. A policy and data quality audit of each state is conducted biennially by the FBI NCIC Audit Staff. A special audit of a CTA should be part of the sanction package.
- 3. Results of the audit are presented to the Sanctions Ad Hoc Subcommittee during the NCIC Advisory Policy Board meeting.
- 4. The Subcommittee is responsible for reviewing the biennial audit of each state and Federal agency accessing the NCIC System.
 - a. The Subcommittee evaluates compliance with NCIC policy, the quality of information placed in the system, and the level of NCIC access provided to local users by the servicing state or Federal agency.
 - b. The Subcommittee is charged with ensuring compliance by all CTAs with NCIC policies.

7/1/92

SAS-23

5. Sanctions currently available to NCIC, the CTAs, Sanctions Subcommittee, Regional Working Groups, and the Board are:

a. Letter of Request for Compliance

- (1) FBI NCIC sends a letter to the CTA officer regarding areas of noncompliance with NCIC policy with a deadline of 45 days to correct the deficiencies.
- (2) The CTA sends a letter to the offending terminal agency regarding this information.

b. Letter of Intent to Remove from the System

- (1) The Board sends a letter to the CTA head if the deficiencies are not corrected.
- (2) The CTA sends a letter to the terminal agency if the deficiencies are not corrected.

c. Advisory Letter to the Governor

- (1) The Sanctions Ad Hoc Subcommittee may send a letter to the governor with a copy to the CTA.
- (2) The CTA should send a letter to the offending terminal agency that the removal of records and/or discontinuance of service is imminent.
- (3) This letter should precede discontinuance of service.

d. Enforcement of Sanctions Pending Reinstatement

- (1) The Board and FBI NCIC jointly initiate the removal of the CTA/state from active system use.

- (2) The CTA may discontinue service to an offending agency and purge that agency's records from state and NCIC files.

e. Reinstatement

- (1) Upon satisfactory proof the offending state has corrected its deficiencies, the Board may reinstate.
- (2) Upon satisfactory proof the offending terminal has corrected its deficiencies, the CTA may reinstate.

VII. CONCLUSION

In summary, the system must be used properly in order for the criminal justice community to obtain the maximum and expected benefits from NCIC.

It is particularly important to remember:

1. In order for NCIC to be an effective communications network, certain **standards** must be established, adopted, and followed, i.e., standards to facilitate the prompt return of responses to its users or the timely entry and removal of records.
2. A failure to comply with NCIC policies, procedures, and standards will subject a state system and other state and local criminal justice users accessing NCIC through the system to various **sanctions** as approved by the NCIC Advisory Policy Board.
3. There are **two ultimate sanctions** available to NCIC management for enforcement of policy and procedure: 1) **purge of an agency's records** and 2) **discontinuance of system access**.

INSTRUCTOR'S NOTE: SHOW "NCIC SYSTEM SECURITY" VIDEO (PLAYING TIME - 8:20 MINUTES). THIS VIDEO REINFORCES THE POINT THAT ADMINISTRATIVE SANCTIONS CAN BE TAKEN AGAINST AN AGENCY FOR FAILING TO INSURE THAT EMPLOYEES COMPLY WITH RULES CONCERNING DISSEMINATION OF NCIC INFORMATION.

BIBLIOGRAPHY

- Federal Bureau of Investigation. FBI Academy. Quantico, VA. Instructors Development Course Manual. Section C, Instructional Objectives, p. 3C. Revised May, 1990.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. NCIC Operating Manual. Section 1 - What Is NCIC?, p. Intro - 3; Section 4 - User Agreement, pp. Intro 36 thru 48; Section 5 - NCIC Standards and Sanctions, pp. Intro - 49 thru Intro - 62. May 31, 1989. Revision 55.
- Federal Bureau of Investigation. National Crime Information Center. Washington, D.C. "NCIC System Security" Video. May, 1991. 8:20 Minutes.
- "National Crime Information Center Audit Manual 1991". Audit Plan, pp. 111 - viii; System Availability, p. 19B.
- "NCIC Staff Paper." Advisory Policy Meeting. June 5-6, 1991. Topic #3 Reformulation of the NCIC Training Curriculum.
- Stuart, Bob. "Bamberg to Employ Dispatcher", The State, October, 1987.
- Stuart, Bob. "Loss of FBI Computer Leaves a Void in Bamberg County Law Enforcement", The State, October 1987.
- U.S. Department of Justice. Federal Bureau of Investigation. Don M. Johnson. "NCIC Training Hit or Miss", FBI Law Enforcement Bulletin, January, 1991. pp. 1-3.
- U.S. Department of Justice. Federal Bureau of Investigation. "Minutes National Crime Information Center Advisory Policy Board." December 8-9, 1982. Audit System. p. 110.
- U.S. Department of Justice. Federal Bureau of Investigation. "Minutes National Crime Information Center Advisory Policy Board." October 17-18, 1984. Subject #12 Publication of State Control Terminal Agency (SCTA) and State Control Terminal Officer (SCTO) Responsibilities into a New Chapter of the NCIC Operating Manual. p. 311.
- U.S. Department of Justice. Federal Bureau of Investigation. "Minutes National Crime Information Center Advisory Policy Board." May 22-23, 1985. Issue: Report on Sanctions Applied. pp. 115-116.

Webster's II New Riverside University Dictionary. The
Riverside Publishing Company. Boston, MA. p. 910.

Webster's New Collegiate Dictionary. G. & C. Merriam
Company. Springfield, MA. p. 1125.

7/1/92

SAS-28

OVERHEAD TRANSPARENCIES

SAS-OH #1-13

NCIC Standards and Sanctions Lesson Plan

7/1/92

NCIC
STANDARDS
AND
SANCTIONS

7/1/92

SAS-OH #1

431

432

DEFINITION OF A POLICY FOR NCIC PURPOSES

**A policy is defined as a plan or course of action
designed to influence and determine decisions and
actions.**

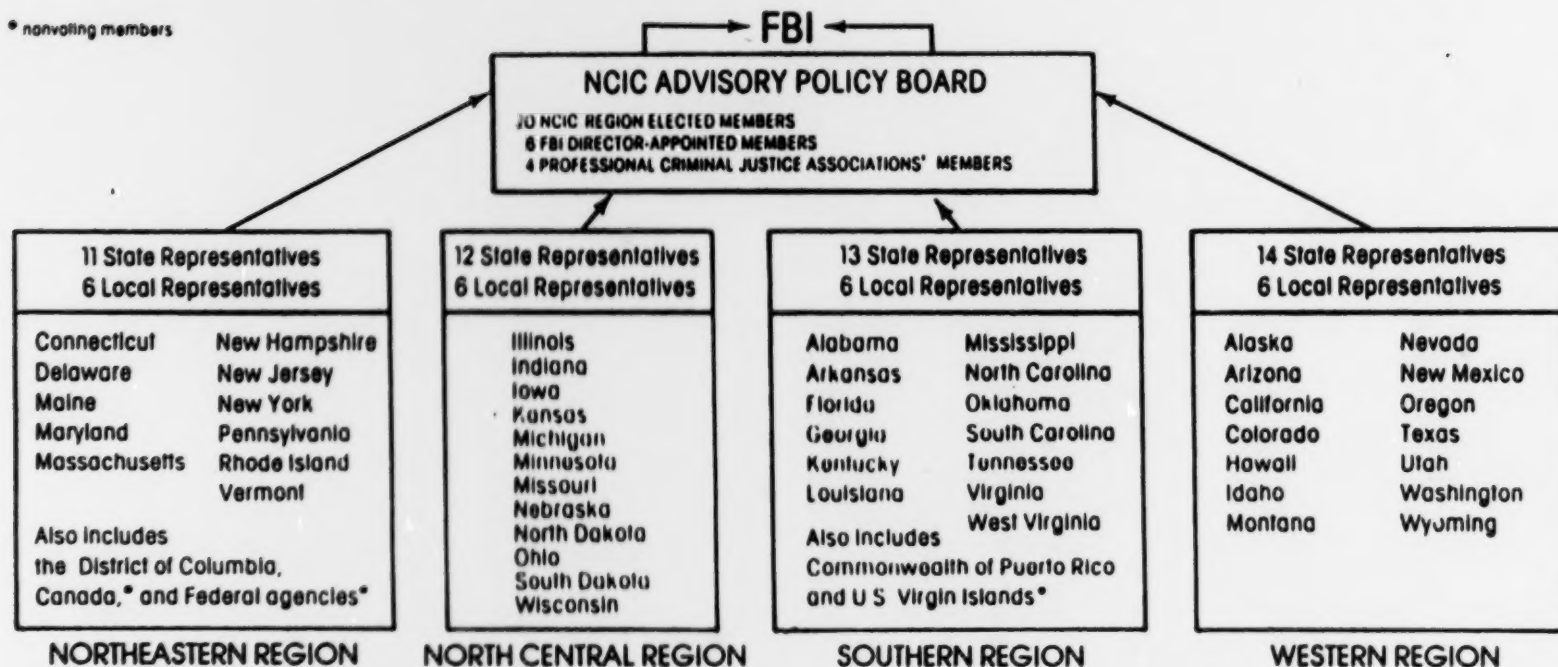
433

7/1/92

SAS-OH #2

434

* nonvoting members



- Responsible for recommending general policy to the FBI with respect to the philosophy, concept, and operational principles of the NCIC.

7/1/92

SAS - OH #3

436

435

AUDIT MANDATE

The Advisory Policy Board stated that by December 31, 1986, each CTA and FSC shall establish a system to biennially (once every two years) audit every terminal agency to ensure compliance with state and NCIC policy and regulations.

7/1/92

437

SAS-OH #4

433

NCIC TRAINING POLICY

The Advisory Policy Board stated that by December 31, 1986, each CTA shall establish a system which will include, but is not limited to*:

1. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.
2. Biennially provide functional retesting and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

* Note: 1. and 2. refer specifically to terminal operators.

TERMINAL AGENCY COORDINATOR (TAC) RESPONSIBILITIES

Each CTO shall ensure that each terminal agency administrator designate an individual to function as a **Terminal Agency Coordinator (TAC)** who shall be responsible for ensuring compliance with state and NCIC policy and regulations including validation requirements.

7/1/92

441

SAS-OH #6

442

DEFINITION OF A STANDARD FOR NCIC PURPOSES

A standard is defined as the minimum level of acceptable performance that must be demonstrated and can be observed or measured.

443

444

7/1/92

SAS-OH #7

DEFINITION OF A STANDARD FOR NCIC PURPOSES (CONT)

**Standards provide a tool of measurement against
which the NCIC Advisory Policy Board can measure
NCIC System performance.**



7/1/92

SAS - OH #7a

446

445

NCIC STANDARDS

- Standards for Inquiry Response Time
- Standards for Record Entry by User Agency
- Standards for Agencies Receiving a Positive Response (Hit)
- Standards for System Availability
- Standards Regarding Equipment and Technology Compatibility
- Standards for Services Availability

447

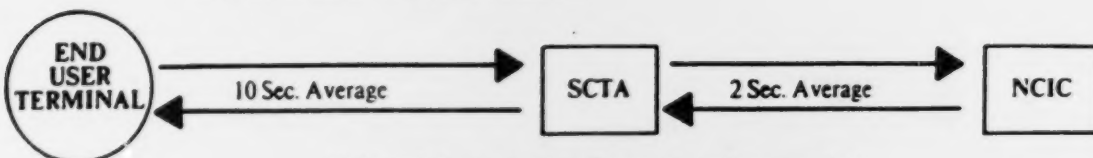
7/1/92

SAS-OH #8

443

INTRODUCTION
SECTION 5--NCIC STANDARDS AND SANCTIONS

EXAMPLE A: NCIC Inquiries - Hot Files
High Speed Lines - Computer Interfaces

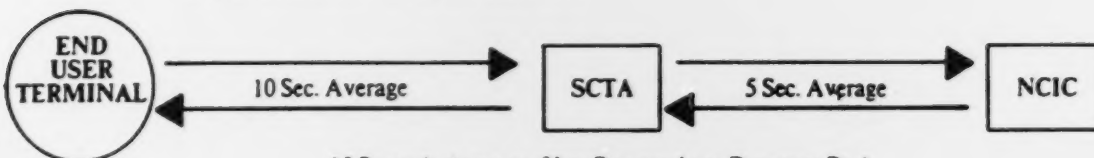


12 Seconds Average - User Request in to Response Back

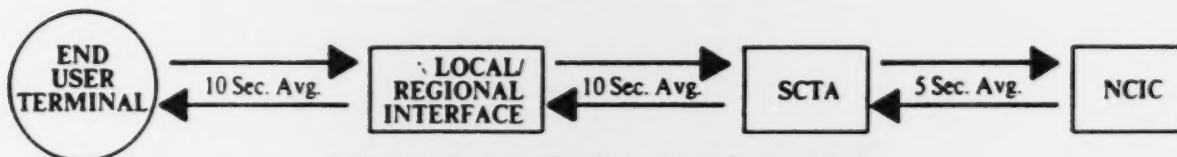


22 Seconds Average - User Request in to Response Back

EXAMPLE B: NCIC Inquiries - III
High Speed Lines - Computer Interfaces

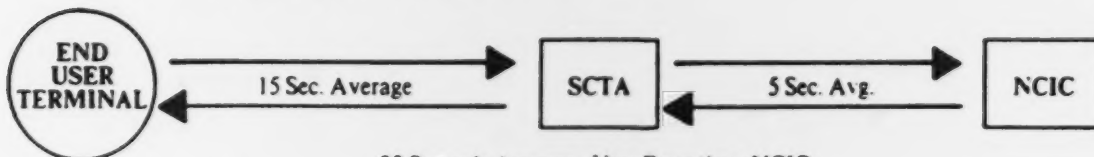


15 Seconds Average - User Request in to Response Back

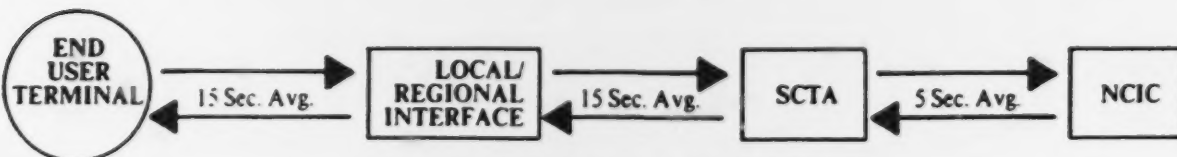


25 Seconds Average - User Request in to Response Back

EXAMPLE C: NCIC Record Entry
High Speed Lines - Computer Interfaces



20 Seconds Average - User Entry into NCIC



35 Seconds Average - User Entry into NCIC

Note: Times shown above should be considered maximum. In many cases, time will be less depending on individual computer systems being used. All times should be considered on an average when all systems are operating normally. Average time should be based upon a compilation over a one month period.

STANDARDS FOR SYSTEM AVAILABILITY – COMPUTER AVAILABILITY GOALS

NCIC COMPUTER - 100% with 99% as minimum acceptable performance

SCTA COMPUTER - 100% with 96% as minimum acceptable performance

LOCAL/REGIONAL COMPUTER - 100% with 96% as minimum acceptable performance

450

7/1/92

SAS-OH #10

451

DEFINITION OF A SANCTION FOR NCIC PURPOSES

A sanction is defined as a penalty, specified or in the form of moral pressure, that acts to ensure compliance or conformity.

452

7/1/92

SAS-OH #11

453

TWO ULTIMATE SANCTIONS AVAILABLE TO NCIC MANAGEMENT

- 1. Purge of an Agency's Records**
- 2. Discontinuance of System Access**

454

7/1/92

SAS-OH #12

455

REASONS WHY SANCTIONS COULD BE IMPOSED

- Failure to React Properly to Hit Confirmation Requests
- Failure to Locate
- Failure to Complete Entries/Modifications/Removals Promptly
- Failure to Make Complete Entries
- Failure to Validate
- Failure to Assure Security of Equipment and Data
- Failure to Provide Trained Operators
- Entry of Invalid or Inaccurate Records
- Failure to Meet Requirements for Training Users of the System
- Failure to Meet Requirements to Biennially Audit Every Terminal Agency

7/1/92

SAS-OH #13

453

457

HANDOUT MATERIALS

SAS-HD #1-7

NCIC Standards and Sanctions Lesson Plan

Loss of FBI computer leaves a void in Bamberg County law enforcement

By BOB STUART
Orangeburg Bureau

BAMBERG

Bamberg County law enforcement officials say they've lost a valuable tool since the county was denied access to the FBI's national crime information computer six weeks ago.

"We can't enter information about stolen merchandise, weapons, criminals, or lost persons in the FBI computer," Bamberg County Sheriff Ed Darnell said Thursday.

Darnell said a county man recently charged with criminal sexual conduct is at large, but without FBI computer access, he cannot notify authorities in other states.

The county's failure to meet state and federal guidelines was cited Oct. 1 when the State Law Enforcement Division informed Bamberg County it could no longer enter data through the FBI computer.

Those guidelines require that the county teletype be monitored 24 hours a day, seven days a week by a licensed dispatcher, said SLED spokesman Hugh Munn.

Munn also said that Bamberg became the state's only county unable to enter information into the FBI computer. It can monitor information in the computer from other places.

Bamberg Mayor Virgil Hicks said SLED had warned county government officials about the problem for the past year.

The teletype, which is housed at the Bamberg City Police Department, is monitored continually by three city dispatchers from 5 p.m. to 8 a.m. on weekdays and all day on weekends and holidays, said Hicks.

He said the teletype is not continually watched during normal weekday hours. Hicks said a city administrative clerk handles dispatching duties from elsewhere in the Bamberg City Hall.

Darnell and Bamberg City Police Chief George Morris have proposed that the county and cities of Denmark and Bamberg centralize dispatching services for one year and fund an extra dispatcher.

Bamberg County already pays \$13,500 a year to the city for dispatching services while Denmark has its own police dispatchers.

County government officials agreed to consider a study of a central police dispatch during a meeting Thursday.

And Denmark Mayor Sam Neeley and County Councilman Isaiah Odom agreed to ask their respective councils to consider funding an additional dispatcher for six months so that the county can regain access to the FBI computer.

Hicks said if the proposal is approved, the county could have its access back before the end of the year.

Reprinted from The State,
October, 1987

SAS-HD #1

Bamberg to employ dispatcher

By BOB STUART
Orangeburg Bureau

BAMBERG

Bamberg County has taken a step toward regaining access to the FBI national computer it lost seven weeks ago.

Bamberg County Council and Denmark City Council voted Monday to appropriate \$4,000 each to fund the hiring of a temporary police dispatcher, who could be hired within a week, said Bamberg City Clerk Mack Clinkscale.

The dispatcher is needed to monitor the county teletype weekdays from 8 a.m. to 5 p.m.

The county's failure to provide around-the-clock, seven-day-a-week teletype monitoring by a dispatcher was cited Oct. 1 when the State Law Enforcement Division informed the county it could no longer enter data into the FBI computer.

Bamberg County was in violation of state and federal guidelines for computer use, said SLED Spokesman Hugh Munn.

Munn said Tuesday that Bamberg County could regain use of the FBI computer once it is in compliance.

The computer is used by law enforcement agencies to exchange information nationwide concerning stolen merchandise, weapons, criminals, and missing persons.

Bamberg County Sheriff Ed Darnell said he and other law enforcement officials are reduced to telephoning out-of-state authorities to give information about crimes committed in the county.

Darnell said the county still can monitor FBI computer information.

Monday's action by the county and city councils also provides that County Council formulate a plan to centralize police dispatching in the county over the next six months, said Denmark Mayor Sam Neeley.

Reprinted from The State,
October, 1987.

SAS-HD #2

AUDIT PLAN

SCOPE

Our system of managing public programs today rests on an elaborate structure of interlocking relationships among all levels of government. Those officials who manage the programs must render a full account of their activities. The requirement for accountability has created a demand for more information about the effectiveness of, and necessity for, government programs. Public officials, legislators, and private citizens want and need to know whether government programs are in compliance with laws and regulations, and whether government organizations are achieving the purposes for which they are authorized and funded.

These standards necessitate an audit system to ensure full accountability and to assist government officials and employees in carrying out their responsibilities.

Three elements may be present in an audit program. These are:

1. Compliance - determines whether the entity has complied with laws and regulations that may have a material effect on the program.
2. Economy and Efficiency - determines whether an agency is managing and utilizing its resources economically and efficiently.
3. Effectiveness - determines whether the desired results or benefits established by the authorizing body are being achieved.

An audit of a government entity may include any combination of these elements. It is not intended, feasible, or desirable that every audit should include all three. An audit including all three aspects should only be conducted when circumstances so dictate.

BASIC PREMISES

The following premises underlie these standards and were considered in their development.

1. The term "audit" is used to describe work done by Auditors in reviewing the program to determine

- a. compliance with applicable laws and regulations
 - b. economy and efficiency of operations
 - c. effectiveness in achieving program results
2. Public officials are accountable to both levels of government for the resources provided to carry out government programs, and to the public. Consequently, they should provide appropriate reports to those to whom they are accountable. In the case of the National Crime Information Center (NCIC), audit results should be provided to the Control Terminal Officer (CTO), and the Advisory Policy Board.
3. Auditors should rely upon the work of other Auditors to the extent feasible if they satisfy themselves as to the other Auditors' independence, capability, and performance through tests or other acceptable methods.

GENERAL STANDARDS

1. Qualifications - The Auditors assigned to perform the audit must collectively possess adequate professional proficiency for the tasks required.
2. Independence - In all matters relating to the audit work, the audit organization and the individual Auditors must be free from personal or external impairments to independence, must be organizationally independent, and shall maintain an independent attitude and appearance. Insofar as NCIC is concerned, audits of the Control Terminal Agency (CTA) should be performed by the FBI, and audits of the individual users should be performed by the CTA.
3. Care Due - Professional care is to be used in conducting the audit and preparing related reports.
4. Reporting - Written audit reports are to be submitted to the appropriate officials of the organization audited and to the appropriate superior of the organization requiring or arranging for the audits unless legal restrictions or ethical considerations prevent it. Copies of the report should also be sent to other officials who may be responsible for taking action and to others authorized to receive such reports. Copies of such audits should be made available for public inspection.

EXAMINATION AND EVALUATION STANDARDS

1. A review is to be made of compliance to applicable laws and regulations.
2. During the audit, a study and evaluation shall be made of the internal control system applicable to the organization, program, activity, or function.
3. General controls in data processing shall be reviewed to determine whether a) the controls have been designed according to management direction and normal legal requirements and, b) the controls are operating effectively to provide reliability of, and security over, the data being processed.
4. The Auditor should review controls of installed data-processing applications upon which the Auditor is relying to assess their reliability in processing data in a timely, accurate, and complete manner.
5. The Auditor shall be alert to situations that could be indicative of fraud, abuse, or illegality; and, if evidence is detected, the Auditor shall take steps to identify the effect on the entities, operations, and programs.

AUDIT REPORT

The audit report shall include a description of the scope and objectives of the audit as well as:

1. A description of material weakness found in the internal control systems, if any.
2. The report should include significant instances of noncompliance with applicable laws, regulations, policies, or procedures and instances of or indications of fraud, abuse, or illegal acts found during, or in connection with, the audit.
3. Recommendations for actions to improve problem areas noted in the audit and to improve operations. The underlying causes of problems reported must be included to assist in implementing corrective actions.

4. Pertinent views of responsible officials of the organization, program, activity, or function audited concerning the Auditors' findings, conclusions and recommendations must be sought. When possible these views should be obtained in writing.
5. A describing of noteworthy accomplishments, particularly when management accomplishments in one area may be applicable to other agencies.
6. A listing of any issues or questions needing further study and consideration.

In all instances the audit report must place primary emphasis on improvement rather than criticism of the past. Critical comments should be presented in a balanced perspective considering any unusual difficulties or circumstances faced by the operating officials concerned.

OBJECTIVES

The audit of the CTAs and Service Coordinators will have four basic objectives. These are:

1. To provide reasonable assurance that the System is in compliance with the legal requirements established by both Federal and state authorities, and NCIC Advisory Policy Board directives.
2. To ensure that the CTA has established suitable systems to provide for managerial control.
3. To provide reasonable assurance that appropriate control systems have been established by the CTA to ensure user compliance with law and policy.
4. To provide reasonable assurance that the CTA has instituted sufficient controls to guarantee that the System provides reliable and accurate information.

In order to ensure that these four objectives are met, the audit will examine five basic areas. These are:

1. General administrative management of the System, including training.
2. Security, including personnel and technical matters.

3. Quality assurance, including State audit mechanisms.
4. System performance.
5. Data quality assessment.

METHODOLOGY

Audits shall be conducted of each CTA and Service Coordinator on a biennial basis. The audit will include a sample of state and local criminal justice agencies to verify compliance.

Specific audit methodology will be as follows:

1. At least 90 days prior to the audit, a listing of audit requirements will be forwarded to the CTA by the NCIC Staff. The list of requirements will include the specific questions and the documentation to be submitted in support of responses. The CTA or Service Coordinator must return the questionnaire to the NCIC Staff, to be received by the Staff, no later than 20 working days prior to the initial date of the audit.
2. Upon receipt of the CTA responses, the NCIC Audit Staff will review the responses for compliance with all applicable Federal law, state law, and policy requirements.
3. The on-site phase of the audit will consist of a review of agency practice to ensure that the agency practice conforms with policy. In addition, the on-site audit of the CTA will include areas that can only be reviewed at the CTA.
4. The Audit Team, using documentation obtained from the CTA and from FBI NCIC, will then audit specific records from a representative number of user agencies. This will ensure that users, as well as the CTA, are in compliance with the laws and regulations.
5. After completion of the CTA and user audit, the NCIC Audit Staff will meet with representatives of the CTA to review preliminary findings.

6. Upon completion of the audit, the NCIC Staff will provide a written audit report, noting any unresolved exceptions. Copies of the report will be provided to the CTO, and the Advisory Policy Board. The original of the audit report will be maintained by the NCIC Audit Staff.



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

September 11, 1991

TO: ALL CONTROL TERMINAL OFFICERS (CTOs) AND FEDERAL SERVICE
COORDINATORS

THIS LETTER, AND THE ATTACHED DOCUMENTATION, MAY
REQUIRE SIGNIFICANT CHANGES TO YOUR NATIONAL CRIME INFORMATION
CENTER (NCIC) TRAINING PROGRAM.

During the December, 1989 meeting of the Advisory Policy Board, the Chairman appointed a Training Ad Hoc Subcommittee to address a number of key training issues that affect all Control Terminal Agencies (CTAs). This letter contains a succinct summary of the deliberations of the Training Ad Hoc Subcommittee and the Advisory Policy Board, and highlights changes in policy.

The Advisory Policy Board has approved a significant reformulation of NCIC training policy as follows (underlining identifies parts of the policy that have been changed):

"(1) Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

"(2) Biennially, provide functional retesting, and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with NCIC policy and regulations.

"(3) Maintain records of all training, testing, and proficiency affirmation.

"(4) Initially (within 12 months of employment or assignment) all sworn law enforcement personnel must receive basic training in NCIC matters to ensure effective use of the System and compliance with NCIC policy and regulation."

"(5) Make available appropriate training on NCIC System use for criminal justice practitioners other than sworn personnel."

"(6) All sworn law enforcement personnel and other practitioners should be provided with continuing access to information concerning NCIC/state systems, using methods such as roll call and in-service training."

"(7) Provide peer level training on NCIC System use, regulations, policy, audits, sanctions, and related civil liability for criminal justice administrators and upper level managers."

"(8) Annually review all curricula for relevancy and effectiveness."

Item number two has been changed in response to a suggestion from a CTO. The CTO noted that the requirement to retrain all terminal operators every two years was a duplicative burden since most terminal operators receive continual, informal, on-the-job training. The initial proposal was to extend the retraining period to three years; however, after much discussion, the Training Subcommittee determined that modification of the policy to require functional retesting and reaffirmation of proficiency every two years would address the problem. By implication, if a terminal operator fails the functional retesting, the operator must be retrained. The Subcommittee also discussed the issue of functional retesting, and noted that the CTO is the proper individual to define functional retesting on the state system. Functional retesting may be administered with or without the use of a terminal.

The requirement to maintain records of all training, testing, and proficiency affirmation remains. It is now number three in the requirements. This is a significant change since it is the intent of the Training Subcommittee and the Advisory Policy Board to limit the duty to maintain individual training records to terminal operators. The CTA still has a duty to ensure that records are kept concerning the training of other individuals using the system, but these records need not be maintained on an individual basis. For example, the CTO must

ensure that an individual record is kept concerning the training and retraining of each dispatcher using NCIC. The record may be kept by the CTA or, if the CTO chooses to decentralize training, by the local agency. Records must be kept concerning training of other individuals, such as sworn officers, but the records need not be kept on an individual basis. For example, if rookie sworn personnel receive training in NCIC matters during their basic school, this fact should be documented by the CTA. It is not necessary maintain documentation concerning each individual officer.

Item four sets a higher standard of training for sworn law enforcement personnel than for other members of the criminal justice community. Item four requires that all sworn personnel must receive basic training. Essentially, sworn personnel must receive formal training during the first 12 months on the job.

Item five addresses other practitioners such as district attorney's, judges, etc.. These individuals must have training made available to them. The CTO may address this requirement by appearing at professional seminars, providing videos, or any other method that will familiarize other practitioners with NCIC and the state system.

Item six eliminates the previous requirement to retrain all sworn personnel and other practitioners every two years. The need to provide continual training has been substituted for the biennial requirement. This may be done through roll-call or similar methods.

In order to address continuing questions, definitions of "full service" and "less than full service" terminal operators were developed. A "full access" or "full service" operator is a terminal operator who may be called upon to perform all NCIC functions. An operator is a "full access" operator if the duties, whether full-time, part-time, or occasional, require the capability to perform the full range of NCIC functions. Any individual, whether sworn or nonsworn, who is a "full access" operator must attend a training program that includes all items specified in the mandatory minimum standards curriculum for terminal operators set forth in this letter.

The "less than full access" operator is any individual who has occasion to use a terminal but who is not required to perform all NCIC functions. A "less than full access" operator must have training that is appropriate to the level of access permitted, a degree of training that may be less than that required for the "full access" operator. A full discussion of the "full access" versus "less than full access" operator is

included in the attached staff paper entitled "Reformulation of the NCIC Training Curriculum."

The second significant change established A MANDATORY MINIMUM CURRICULUM FOR "FULL-SERVICE" TERMINAL OPERATORS. All state training programs must include each of the following items in their training curriculum for full service operators:

I. SYSTEM HISTORY

- A. Description of NCIC - organizational authority
- B. Purpose of the System
- C. Authorized User Agencies
- D. Available Files

II. SHARED MANAGEMENT CONCEPT

- A. Goal
- B. Purpose
- C. Advisory Policy Board
- D. Regional Working Groups

III. INTERRELATIONSHIP OF STATE AND NCIC SYSTEM (IF APPLICABLE)

- A. Duplicate Entries
- B. Different Criteria

IV. NCIC AND STATE FILES

- A. Available Files
- B. Criteria
- C. Inquiry, Entry, Modify, Clear, Cancel & Locate Capabilities
- D. Cross Search (\$M, \$N)
- E. Interpreting Responses
- F. Specialized Searches

V. HIT CONFIRMATION

- A. Definition of a Hit
- B. Probable Cause
- C. Ten-minute Hit Confirmation Policy
- D. Confirming a Hit

VI. SYSTEM SECURITY

- A. Physical Security of Terminal and Printouts
- B. Confidentiality
- C. Access Eligibility
- D. Dissemination

VII. INTERSTATE IDENTIFICATION INDEX

- A. Description
- B. How to Use/Criteria for Entry
- C. Permissible Uses
- D. Manual Files
- E. Logging Requirements/Use of Attention Field
- F. Privacy/Security Interests
- G. Purpose Codes
- H. Primary/Secondary Dissemination
- I. Liability

VIII. QUALITY CONTROL

- A. Responsibilities
 - 1. Federal and State
 - a. Automatic Computer Edits
 - b. Automatic Purging of Records

- c. Quality Control (e.g. Serious and Form Errors, Trends and Administrative Messages)
 - d. Validations
 - 2. Entering Agencies - Record Quality
 - a. Timeliness
 - b. Accuracy
 - c. Completeness/Packing the Record - Sources

IX. VALIDATION REQUIREMENT

- A. Definition
- B. Local Agency Procedures for Validating as it Relates to the Terminal Operator
- C. Penalties for Failure to Validate Records

X. STANDARDS AND SANCTIONS

- A. State and Federal Audits
- B. Sanctions Program
- C. Testing and Proficiency Affirmation

XI. LIABILITY

- A. III
- B. Hit Confirmation
- C. Data Quality/Validation

XII. DOCUMENTATION

- A. Entries
- B. Hits
- C. Validations

The NCIC Training Staff is preparing a lesson plan for each of the twelve sections set out in the mandatory minimum curriculum. USE OF THESE LESSON PLANS WILL BE OPTIONAL; however,

each item in the minimum curriculum must be addressed in the state program.

The third change involved creation of a RECOMMENDED MINIMUM TRAINING REQUIREMENT for sworn personnel. This is a suggested curriculum, not mandatory.

I. FILES

- A. Provide a Working Knowledge of All NCIC/State Files (Including Criteria for Entry, Complete Utilization of Fields, Importance of III, etc.)

II. PACKING THE RECORD

- A. Familiarization with Available Resources to Place Complete and Accurate Information into the System

III. DISSEMINATION

- A. Restrictions on Use of NCIC Data (Including III)

IV. DOCUMENTATION

- A. Proper Record Keeping

- 1. Case File
- 2. 2nd Party Check

V. HIT CONFIRMATION

- A. 10-Minute Policy
- B. Probable Cause
- C. Extradition Matters

VI. INVESTIGATIVE ASSISTANCE

- A. Specialized Searches
 - 1. State Capabilities
 - 2. Federal Capabilities

VII. LIABILITY

- A. Data Quality
- B. Validation

A full discussion of the issue of "who is a practitioner" and the degree of training required is included in the attached staff paper.

The issue of "certification" versus "affirmation of proficiency" was discussed by the Subcommittee in detail. The Subcommittee reemphasized the fact that the Advisory Policy Board rejected certification as an NCIC requirement in favor of the term "affirmation of proficiency." States have wide latitude in developing the method used to affirm proficiency. The CTO may require certification as part of state policy.

The attached staff paper includes a discussion and rationale of the changes in the NCIC training policy. It addresses many frequently asked training questions, and attempts to erase misunderstandings that have developed since implementation of the training policy in 1984.

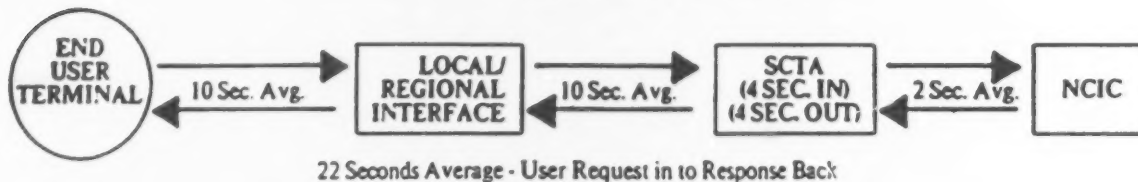
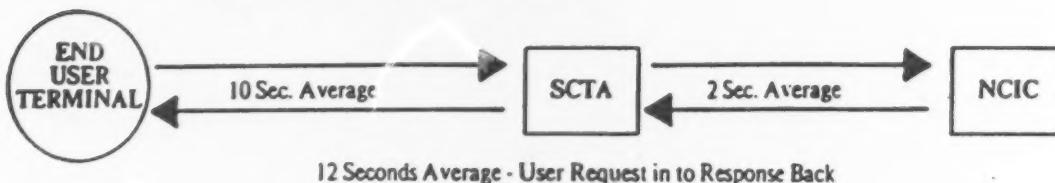
For your information, the NCIC Audit Staff is currently amending the audit protocol to include the mandatory minimum curriculum as a part of the audit review. The Audit Staff will use the attached staff paper as their "policy bible" during future audits. While the staff paper is lengthy, a thorough review should answer any questions that you might have concerning the intent of the Board and the approach to be taken by the Audit Staff. Should you have any questions on the policy, please call Dave Mitchell at 202-324-2608.

Sincerely,

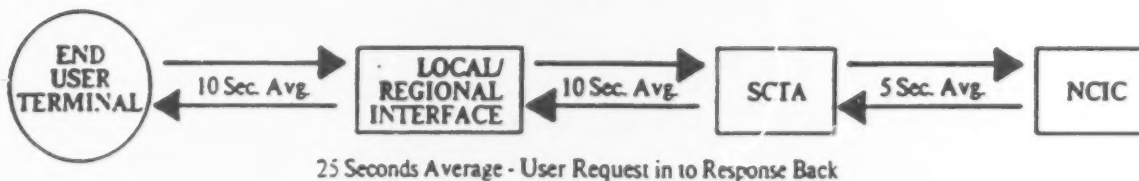
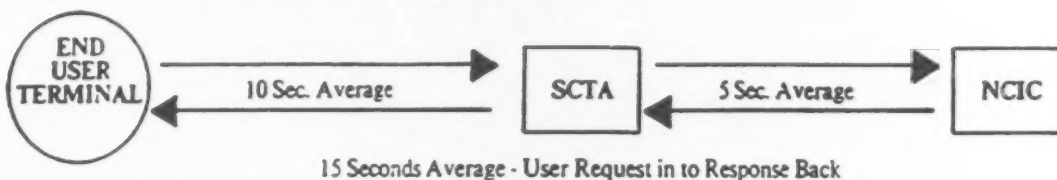
David F. Nemecek
Chief
National Crime Information Center

INTRODUCTION
SECTION 5--NCIC STANDARDS AND SANCTIONS

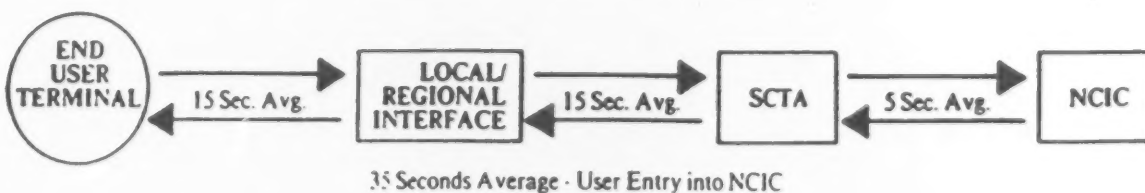
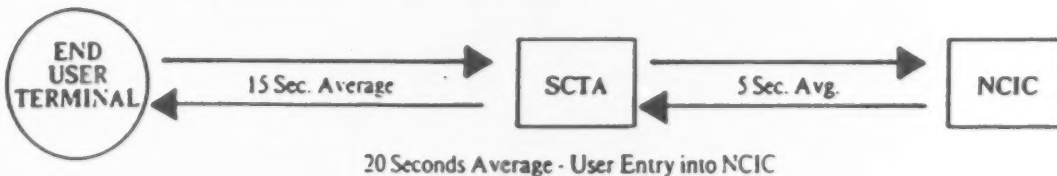
EXAMPLE A: NCIC Inquiries - Hot Files
High Speed Lines - Computer Interfaces



EXAMPLE B: NCIC Inquiries - III
High Speed Lines - Computer Interfaces



EXAMPLE C: NCIC Record Entry
High Speed Lines - Computer Interfaces

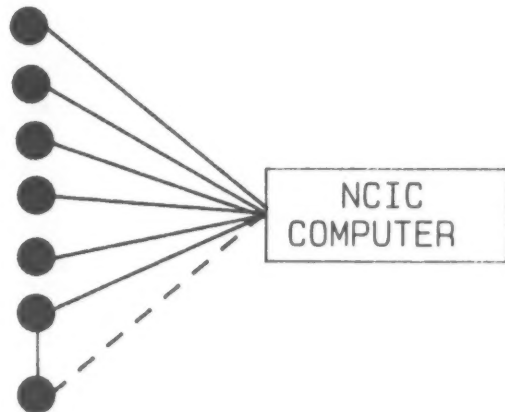


Note: Times shown above should be considered maximum. In many cases, time will be less depending on individual computer systems being used. All times should be considered on an average when all systems are operating normally. Average time should be based upon a compilation over a one month period.

Current NCIC System

INFORMATION BASES

YEAR OF IMPLEMENTATION



NCIC
COMPUTER

37,309 Law Enforcement
33,878 Other Criminal Justice

71,187 Total Authorized Users

STOLEN VEHICLES	1967
STOLEN ARTICLES	1967
STOLEN OR RECOVERED GUNS	1967
STOLEN LICENSE PLATES	1967
WANTED PERSONS	1967
STOLEN SECURITIES	1968
STOLEN BOATS	1969
MISSING PERSONS	1975
INTERSTATE IDENTIFICATION INDEX	1983
U.S. SECRET SERVICE PROTECTIVE	1983
UNIDENTIFIED PERSONS	1983
ORIGINATING AGENCY IDENTIFIER	1985
FOREIGN FUGITIVE	1987
ATF VIOLENT FELON FILE	1992

NATIONAL CRIME INFORMATION CENTER

USER AGREEMENT

USER AGREEMENT

Responsibilities of Control Terminal Officer (CTO) in the National Crime Information Center (NCIC) System

I. Introduction

Since its inception, the NCIC has operated under a shared management concept between the FBI and state users. The NCIC Advisory Policy Board established a goal of having a single state agency in each state assume responsibility as the NCIC Control Terminal Agency (CTA) for the state, through and by which NCIC users in that state would access NCIC. The CTA is responsible for planning for necessary hardware, software, funding, and training for complete access to NCIC data services by all authorized agencies within the state.

The Board approved the CTA concept in order to unify responsibility for system user discipline, and adherence to system procedures and policies within each state. The CTA also serves as a central point in its state for handling record validations, quality control matters, dissemination of manuals and other NCIC publications, security matters, user training, audit, and any other problems concerning system use that may arise.

FBI NCIC responsibilities under this shared management concept includes provision of:

- operational, technical, and investigative assistance to NCIC users;
- telecommunications lines to a state interface;
- legal and legislative review of matters pertaining to NCIC;
- timely information on all NCIC aspects of system usage by means of the NCIC Operating Manual, Technical and Operational Updates, and related documents;
- staff research assistance;
- training and training materials to the control terminal agencies.

The responsibilities of the CTO and NCIC Service Coordinators (SC) are detailed in several documents related to the NCIC System. This agreement outlines the varied responsibilities of a CTO/SC as they pertain to the NCIC System.

The following documents are incorporated by reference and made part of this agreement:

- (A) National Crime Information Center Operating Manual.
- (B) NCIC Computerized Criminal History (CCH) Program Background, Concept and Policy as amended or superceded by implementation of the Interstate Identification Index (III) Program.
- (C) Minutes of the NCIC Advisory Policy Board.
- (D) Bylaws for the NCIC Advisory Policy Board and Regional Working Groups.
- (E) Title 28, Code of Federal Regulations, Part 20.
- (F) NCIC Standards as recommended by the NCIC Advisory Policy Board and approved by the FBI Director.
- (G) Applicable Federal and state law and regulation.

II.

Definitions

Control Terminal Agency

A CTA is a state or territorial criminal justice agency on the NCIC System providing statewide (or equivalent) service to its criminal justice users with respect to NCIC data. Only those agencies with direct telecommunications lines to NCIC may be control terminal agencies, and are held responsible for records entered through those lines. There will be no more than one CTA per state or territory.

NCIC Control Terminal Officer and Service Coordinator

An NCIC CTO shall be appointed by the head of each CTA.

An NCIC SC shall be non-CTAs which have direct NCIC telecommunications lines, which lines will be used only for system query functions.

The CTO will be allowed sufficient time to perform all necessary duties related to NCIC responsibilities. The CTO/SC and his agency will be responsible for

monitoring system use, enforcing system discipline, and assuring that NCIC operating procedures are followed by all users of the respective NCIC telecommunications lines as well as other related duties as outlined by this agreement. When a new CTO or SC is designated, the CTA head will notify NCIC of that appointment within 10 days of the appointment.

Timeliness

NCIC records must be entered promptly to insure maximum system effectiveness. A timely entry in the Wanted Person File is one made immediately once:

1. The decision to arrest or authorize arrest has been made; and,
2. The decision has been made as to whether and how far to go for extradition.

The date of want or date of warrant must be the date on which all those decisions were made.

A timely removal from the file means an immediate removal once the originating agency has documentation the fugitive has been arrested or is no longer wanted. Timely system inquiry means initiation of the transaction before an officer begins writing an arrest or citation document of any kind; storing inquiries when NCIC is down and submitting them at once when the system returns, regardless of whether the subject is still in custody; inquiry prior to the release of a person who has been incarcerated; and inquiry upon those who appear at a custodial facility to visit inmates.

Timeliness of entry/modification in the Missing Person File is generally the same as in the Wanted Person File.

Timely entry/modification of vehicle, license plate, and vehicle part data matches the wanted person standard, less the extradition considerations. Entry should be made as soon as a cross-checking with Motor Vehicles Registration Files has been completed.

Timely entry of gun, article, and securities information means within a few hours of the time complete information is available.

Validation

Validation (vehicles, plates, fugitives, missing person entries) obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation procedures are defined in Section IV-C of this agreement.

Completeness

Complete records of any kind include all information that was available on the person or property at the time of entry. The validation process should include a review of whether additional information has become available (missing from original entry) that could be added.

Complete inquiries on persons include numbers that could be indexed in the record; i.e., Social Security, Passport, VIN, License Plates, Driver's License, etc. Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

Accuracy

The accuracy of NCIC data must be double-checked by a second party. That verification should include assuring that the available cross-checks (VIN/license numbers) were made, and that data in the NCIC record matches the data in the investigative report. Agencies lacking support staff for this cross-checking should require the case officer to check the record, as he carries primary responsibility for seeking the fugitive and the stolen property.

III. Operational Responsibilities of Control Terminal Officers and Service Coordinators

To help ensure the proper operation of NCIC, the standards, procedures, formats, and criteria as contained in the NCIC Operating Manual will be followed. The CTA and its officers and their agencies with direct NCIC lines and their NCIC SCs must not only follow the rules as set forth, but also must ensure that agencies served by the control terminal do the same. Specific actions relative to two operational situations are:

(A) Ten Minute Hit Confirmation Policy

An originating agency must within ten minutes furnish to an agency requesting a record confirmation, a response indicating a positive or negative confirmation or a notice of the specific amount of time necessary to confirm or reject.

This confirmation policy is especially critical with regard to a hit in the Wanted Person File. The NCIC Operating Manual describes procedures for handling a Wanted Person File hit in Part 7, Section 5.6. When an agency receives a hit on a wanted person record, it is requested by a caveat to "IMMED CONFIRM WARRANT AND EXTRADITION WITH ORI." Confirming the hit means to verify with the ORI that the subject of the inquiry is identical to the subject in the record received, if the warrant is still outstanding, and whether or not the individual will be extradited. Upon receipt of a hit confirmation request, the originating agency must, within ten minutes, furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject. Therefore, in instances where the extradition information is not readily available, the originating agency should advise the inquiring agency, within ten minutes, that such is the case and how much time will be necessary to obtain the information.

An agency requesting confirmation which fails to receive a response to the first request shall generate a second request with a copy to its CTO or SC and to the CTO or SC of the state in which the agency holding the record is located.

A CTO or SC designee of a system which services an originating agency of a record will institute appropriate action to ensure proper response to a hit confirmation request and to comply to system standards. This appropriate action may include canceling the record by the CTA.

Failure of a CTA to ensure compliance with this policy will result in imposition of sanctions as approved by the NCIC Advisory Policy Board.

(B) Control Terminal and/or NCIC Line Failure

Operational failure at the user end of an NCIC line may result from one of four conditions: (1) the NCIC computer is out of service; (2) the terminal equipment fails or is out of service; (3) a circuit or NCIC line problem; or (4) malfunction of terminal equipment. A terminal should make every effort to verify that the difficulty does not lie within its equipment. The CTA or SC should take the following action when in an out-of-service status and an analysis determines that the problem is not control terminal equipment difficulty: notify the local vendor providing communication service, log the time of notification, and note the circumstances relating to the problem. If, after a reasonable period of time, the vendor's efforts have not resolved the problem, notify FBI NCIC Headquarters and furnish the time the vendor was notified and a brief description of the problem.

IV. Quality Assurance Responsibilities

(A) Introduction

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. However, a CTA assumes a large degree of administrative responsibility and possible legal liability for

the maintenance of a criminal justice information system. This responsibility is being further defined by the courts. Accordingly, the CTA should institute appropriate and reasonable quality assurance procedures for all state system users. It appears from the cases reviewed that the courts have specifically addressed the issue as to whether criminal justice information system administrators (i.e., CTO and agency head) can be held liable for the negligent mishandling of a criminal justice record. In relation to 42 United States Code 3771, there is a standard which is prescribed for record management and (perhaps) the establishment of maintenance standards for these records. It can be said that criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up to date. To ensure reasonably sufficient record management, each CTA should ensure that there are security standards, audit standards, and personnel training standards which would allow accurate and up-to-date records and dissemination of the same.

(B) Record Quality

Errors discovered in NCIC records are classified as serious errors, form errors or an error trend.

- (1) Serious errors: NCIC will advise the CTA and the ORI via teletype message of an apparently erroneous record and request that it be verified, changed or canceled within 24 hours. If neither a response is received nor corrective action taken during that time, NCIC will cancel the record.
- (2) Form error or error trend: NCIC will mail a letter to the appropriate CTA. The CTA will forward a copy of the letter or a similar letter to the ORI so corrective action can be taken. No further notification or action will be taken by NCIC.

(C) Record Validation

NCIC periodically prepares listings of records on file for validation purposes. Validation listings are prepared pursuant to a schedule as published in the NCIC Operating Manual. These listings are mailed to the appropriate control terminals who in turn disseminate the records to the originating agency.

Each CTO will receive a letter explaining what records are contained in the validation, the order in which records are listed, and general procedures for validating the records. Also included are two letters which are to be executed by the NCIC CTO. One letter is used to acknowledge receipt of the validation material. This acknowledgment letter must be returned to FBI NCIC immediately. The second letter is for the CTO to certify that the records have been validated or that certification of validity has been received from the originating agencies.

Validation certification means that: (1) the records contained on the validation listing have been reviewed by the originating agencies; (2) the records which are no longer current have been removed from NCIC and all records remaining in the system are valid and active; (3) all records contain all available information; and (4) the information contained in each of the records is accurate.

This certification letter must be returned to the NCIC within 75 days from the date that the NCIC mailed the validations to the CTA.

If a CTA has not received a certification response from an agency under its service jurisdiction within a specified period of time, the CTA shall purge from NCIC all records which are the subject of that agency's validation listings. If a CTA fails to certify any validation listing to the NCIC within the specified time, all unvalidated records from that state will be purged by the NCIC.

V. Security Responsibilities

(A) General

The data stored in NCIC is documented criminal justice information and this information must be protected to ensure correct, legal and efficient dissemination and use. Information can be obtained from NCIC both directly and indirectly. Direct access is defined as terminal access and dissemination within that terminal agency. Indirect access is nonterminal access outside of an agency with direct access.

There is no Federal legal or policy prohibition against indirect dissemination of information contained in NCIC, other than criminal history record information. If no state/local law or policy prohibition exists, indirect dissemination of NCIC records, other than criminal history record information, is discretionary with the CTA. Such information may be withheld because of criminal justice priorities, budgetary limitations, or other reasons determined to be legitimate by the CTA.

An agency participating in the NCIC as a CTA and other agencies with direct telecommunications line access must assume responsibility for and enforce system security with regard to all other agencies which it in turn services.

Security guidelines relating to criminal history record information are set forth in the NCIC CCH Program Background, Concept and Policy as superseded by the III Program and in Title 28 Code of Federal Regulations Part 20, Subparts A and C.

(B) Originating Agency Identifier (ORI)

An NCIC ORI is a nine character identifier assigned by FBI NCIC to an agency which has met the established qualifying criteria for ORI assignment to identify the agency in transactions in the NCIC System. The assignment of an ORI to an agency is not a guarantee of access to the NCIC System. The ultimate decision regarding who may access NCIC lies with the CTA.

A CTO shall coordinate the assignment of new ORI numbers, the change in ORI location or address, any other changes, cancellations, or retirements of ORIs accessing NCIC through the CTA system with the FBI NCIC. The CTO will submit necessary documentation when requesting the assignment of an ORI. This documentation should include a statute or executive order which indicates an agency is governmental and performs the administration of criminal justice. A statement should be included that indicates that an agency allocates more than 50% of its annual budget to the administration of

criminal justice. If the agency is under the management control of a criminal justice agency, a copy of the management control agreement should be submitted. Assignment of ORIs to agencies with special or limited NCIC access will also be coordinated by the respective CTOs.

Validation

Each ORI accessing NCIC shall be validated on a biennial basis by the CTO. A printout containing ORIs of agencies accessing NCIC through the state system is forwarded to the CTO who shall check the accuracy of each ORI listing to include verification of:

- agency type code.
- agency name and locality.

The CTO shall certify that all ORIs are valid and correct as listed.

VI. Computerized Criminal History Record Information Responsibilities

- (A) Each CTA shall conform with system policy as established by the NCIC Advisory Policy Board and approved by the FBI Director before being permitted access to criminal history record information. This conformity will allow for control over the data and give assurance of system security.
- (B) Each CTA is responsible for the security throughout the system being serviced by that agency, including all places where terminal devices are located. Upon determination that a terminal is in nonconformance with system management or security policy, the CTA shall cause that terminal's access to NCIC to be disabled.
- (C) A system security officer shall be designated in each CTA to assure all necessary physical, personnel, computer, and communication safeguards prescribed by the Board are functioning properly in systems operations.
- (D) The rules and procedures governing direct terminal access to criminal history record information shall apply equally to all participants to the system, including the state CTAs and SCs, Federal SCs, and other agencies having access to the data stored in the system.

- (E) All CTAs and other criminal justice agencies having direct access to computerized CHRI data from the system shall permit an NCIC audit team to conduct appropriate inquiries with regard to any allegations of security violations.
- (F) The CTA shall define procedures to ensure all satellite computers and all remote terminals accessing criminal history record information through the state system will maintain a manual or automated dissemination log with notation of the individual making the request for the record. All logs will be maintained for a minimum of one year.
- (G) A CTA will ensure that all computers and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history record information must be under the management control of a criminal justice agency as defined by the NCIC CCH background and policy document.

All CTAs and SCs should institute a program of systematic self-audits as a means of guaranteeing the completeness and accuracy of information in the system. These self-audits should be on a continual basis to ensure both quality assurance and compliance with standards.

In addition to audits conducted by all CTAs and SCs, each CTA/SC shall be audited at least once every two years by the NCIC Staff. This audit shall include a sample of state and local criminal justice agencies. The objective of this audit is to verify adherence to NCIC policy and regulations and is termed a compliance audit. In order to assist in this audit, each CTO and SC will respond to a preaudit questionnaire which will serve as the audit guideline. A compliance audit may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance.

Such compliance audits shall cover the following areas in connection with both the III and NCIC stolen property and person records:

Accuracy

That any NCIC entry shall contain no erroneous data. In addition, CTAs/SCs should maintain necessary documentation as required by

NCIC policy. They should also ensure that documentation is available from state and local users accessing NCIC through them.

Completeness

That information contained in an NCIC entry or in a criminal history record to be disseminated is all the pertinent available information.

Timeliness

That entry, modification, update, and removal of information are completed as soon as possible after information is available and that information is processed and transmitted in accordance with standards as established by the Board.

Security

The ability of an organization to protect its information against unauthorized access, ensuring confidentiality of the information in accordance with laws and with NCIC policy, regulations, and standards.

Dissemination

That all information released is in accordance with applicable laws and regulations and that a record of dissemination of criminal history records is maintained.

In addition, CTAs/SCs should also ensure that documentation is available from state and local users to assist in both the self-audit and national audit programs.

VII. Administrative Responsibilities

- (A) Each state CTO shall serve as a representative of his/her state to the Regional Working Group (RWG) meetings. The state CTO may designate someone in his/her state to attend and vote at the RWG meetings.

The state CTO shall provide to the RWG chairperson, upon request, a list of those items pertaining to the operation of the NCIC System as well as suggestions for improvement in the operations of the NCIC System which may require discussion at the RWG meetings.

Consistent with each CTO's responsibility to represent the users of that state, he/she should distribute those items on the agenda to be discussed at a RWG meeting to appropriate state and local users to ensure that all views on the topics are obtained and represented. In addition, he/she should be prepared to fully discuss those agenda items at the RWG meetings.

- (B) The CTO shall cooperate, to the maximum extent possible consistent with any fiscal, time, or personnel constraints, in the response to requests for information in the form of surveys, questionnaires, or similar methods, which may be provided by FBI NCIC from time to time.
- (C) The CTO shall be responsible for providing adequate training to agencies accessing NCIC through the state CTA computer.
- (D) The CTO shall ensure that publications emanating from FBI NCIC be distributed to appropriate personnel in that state. Consistent with this provision, the CTO shall coordinate distribution within their state criminal justice community of the NCIC Technical and Operational Update, NCIC Operating and Code Manuals, and, as requested, miscellaneous publications in order to enhance effective use of the NCIC System.

ACKNOWLEDGMENT

As a CTA/SC serving in the NCIC System, we hereby acknowledge the duties and responsibilities as set out in this document as well as those documents incorporated by reference. We acknowledge that these duties and responsibilities have been developed and approved by NCIC System users in order to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the NCIC System. We further acknowledge that a failure to comply with these duties and responsibilities will subject my state system and those other state and local criminal justice users accessing NCIC through that system to various sanctions as approved by the NCIC Advisory Policy Board. These sanctions may include the termination of NCIC services to the CTA.

Control Terminal Officer Date

Control Terminal Agency Head Date

Daniel B. Henneke

Chief, FBI NCIC

Date

The network philosophy of the State Control Terminal Agency (SCTA) is a sound one but has not been fully implemented. The negative result of this delayed implementation has been counter to the expressed NCIC purpose to "help the criminal justice community" perform its duties. In effect, certain cities in our present network configuration are being helped to the disadvantage of the SCTA; and indirectly are being helped to the disadvantage of other agencies nationwide that must rely on the SCTA system to enforce discipline.

Effective operation of the NCIC System and effective communications throughout the networks within each state are not possible under the present condition. Criminal justice agencies cannot rely on the present design to aid them in ensuring that their communications have followed all the necessary channels in the most effective manner. Most SCTAs have and/or have access to more data files than are available in NCIC. For example, in addition to forwarding wanted person inquiries to NCIC, SCTAs also search state wanted files to obtain misdemeanor warrant entries which do not qualify for entry in NCIC. Some SCTAs forward stolen vehicle inquiries to NCIC, state vehicle files, and computerized motor vehicle registry files and provide the inquiring officer with not only the results of the stolen check, but also the name, address, etc., of the registered owner. Some SCTAs may carry the last example another step and provide the officer with any warrants issued for the registered owner. Thus, the use of a direct line between the NCIC System and a city/regional system also results in the criminal justice officer losing services which are available at, and provided by, only the SCTA.

System discipline, standards, management, and control are subverted by the present fragmented arrangement and the result hinders interagency cooperation.

The use of "effective communications" to help the criminal justice community perform its duties not only means providing access to and detailed information from pertinent computerized data bases, but also includes the amount of time required to access the data bases. While an entry, inquiry, or update message may contain specific and detailed information, the message (communication) could be very ineffective if it cannot be transmitted to the data center, and a response received from the data center within a reasonable amount of time. It is not uncommon to hear of a hit occurring minutes after the record was entered. Restrictions have also been placed on the amount of time that a person may be detained while an inquiry is being made to determine whether a record is on file in a data base. The rapid transmission of messages is extremely important and the standards

were prepared to ensure that messages are transmitted and processed within a reasonable amount of time.

Neither the NCIC System nor the state networks will ever be able to reach their maximum potential as criminal justice tools until all the necessary components are working toward that end. Until then the effectiveness of the entire effort is diminished.

There are currently a number of NCIC lines which go directly to city and regional computer systems and FBI field offices. Many of these direct lines have a very low volume of traffic. In these times of fiscal constraints, unnecessary and/or exorbitant costs are inexcusable. Under what situations do direct lines to city/regional systems exist? Study reveals that, while many situations may first appear to be unique, the reasons in fact can be categorized into one or more of the following areas of complaint:

1. Satisfactory response time is not provided by the SCTA.
2. System availability is not satisfactory.
3. Some services provided by NCIC are not available through the SCTA.
4. Equipment and/or technical methods are incompatible with the SCTA.

Reaching the objective to provide the most reasonably effective communications network for all criminal justice agencies will not be possible unless the direct lines to city/regional systems and FBI field office arrangements are eliminated and the needs of everyone involved are properly met.

To accomplish this objective the establishment of certain policies and standards must be completed, adopted, and followed. Through these policies and standards a tool of measurement will be provided against which the Advisory Policy Board can measure the performance of the component parts of the system as a whole. These policies and standards also must address the specific areas of complaint of the "special" case situations.

For the purposes of the standards on the following pages, any 1200 or higher baud line shall be considered a high-speed line.

STANDARDS FOR INQUIRY RESPONSE TIME - HOT FILES (NON-III)
High-Speed Line - Computer Interface

1. Average message response time for an inquiry from the SCTA to NCIC and back to the SCTA should not exceed two seconds.
2. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 12 seconds after transmission of the inquiry, with two of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1 above.
3. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 22 seconds after the transmission of the inquiry, with 12 of the 22 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 1 and 2.
4. Average response time from any local/regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 12 seconds, with two of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1.
5. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the inquiry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 12 second response time indicated in standard 2 above.

Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the one-month compilation.

STANDARDS FOR RESPONSE TIME (III)
High-Speed Line - Computer Interface

1. Average message response time for an inquiry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.
2. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 15 seconds after transmission of the inquiry, with five of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1 above.
3. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 25 seconds after the transmission of the inquiry, with 15 of the 25 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 1 and 2.
4. Average response time from any local regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 15 seconds, with five of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 1.
5. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the inquiry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 15 second response time indicated in standard 2 above.

Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as the installation of a new computer, should be excluded from the one-month compilation.

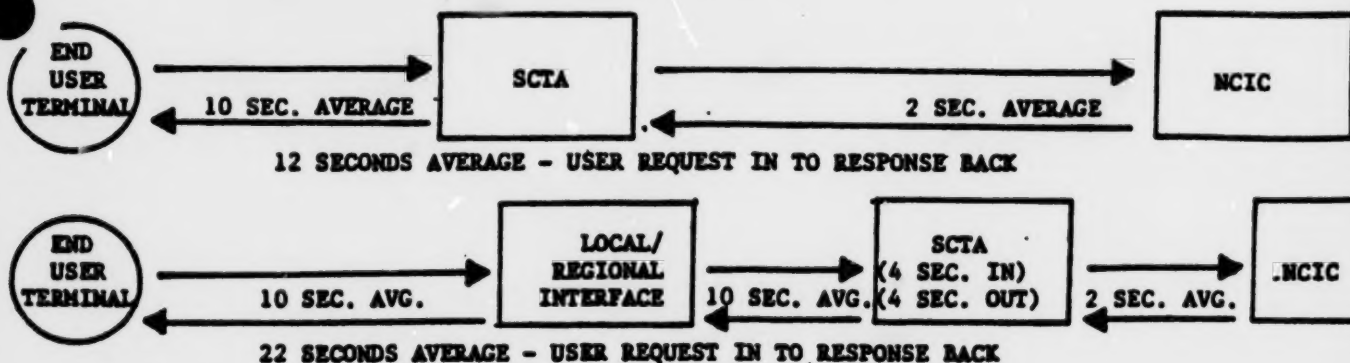
STANDARDS FOR RECORD ENTRY BY USER AGENCY

1. Any agency having investigative authority and jurisdiction and having an NCIC-assigned Originating Agency Identifier (ORI) must enter records into NCIC which meet NCIC criteria as soon as reasonably possible after minimum information is available.
2. The SCTA shall be responsible for assuring that every agency which has a terminal or access to a terminal by some interagency agreement and has an NCIC-assigned ORI and investigative authority and jurisdiction may enter records into NCIC.
3. Every agency which enters records destined for NCIC must assure that "hit" confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location.
4. Every agency is responsible for the removal of its NCIC record as soon as it is aware that the record is no longer valid.
5. Average message response time for an entry from the SCTA to NCIC and back to the SCTA should not exceed five seconds.
6. Average message response time from an SCTA to an agency interfaced with the SCTA should not exceed 20 seconds after transmission of the entry, with five of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 5 above.
7. Average message response time for an end user terminal interfaced with a local/regional system which is interfaced with an SCTA should not exceed 35 seconds after the transmission of the entry, with 20 of the 35 seconds allocated to the transmission to, processing by, and return of the response from the SCTA and NCIC as described in standards 5 and 6.
8. Average response time from any local/regional system or terminal interfaced directly with the NCIC computer (i.e., NCIC lines which terminate at an agency that is not an SCTA) to an end user terminal interfaced with the local/regional system shall not exceed 20 seconds, with five of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC as described in standard 5.

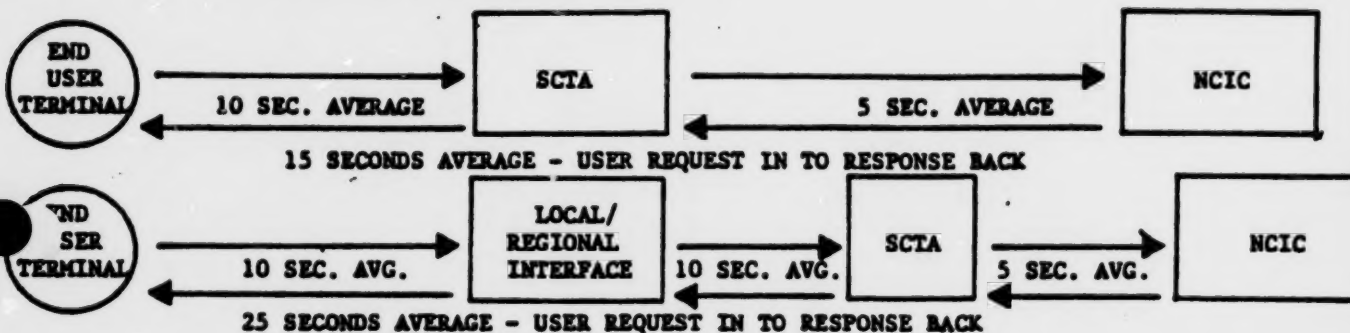
9. The times indicated in the above standards are for high-speed lines only. An additional 10 seconds should be added to the above times for each low-speed line interface, with five seconds allocated to the entry and five seconds to the response. For example, if an end user terminal is interfaced with an SCTA via a low-speed line and the SCTA is interfaced with NCIC via a low-speed line, an additional 20 seconds would be added to the maximum 20 second response time indicated in standard 6 above.

Standards for record entry into NCIC for processing are shown in Example C.

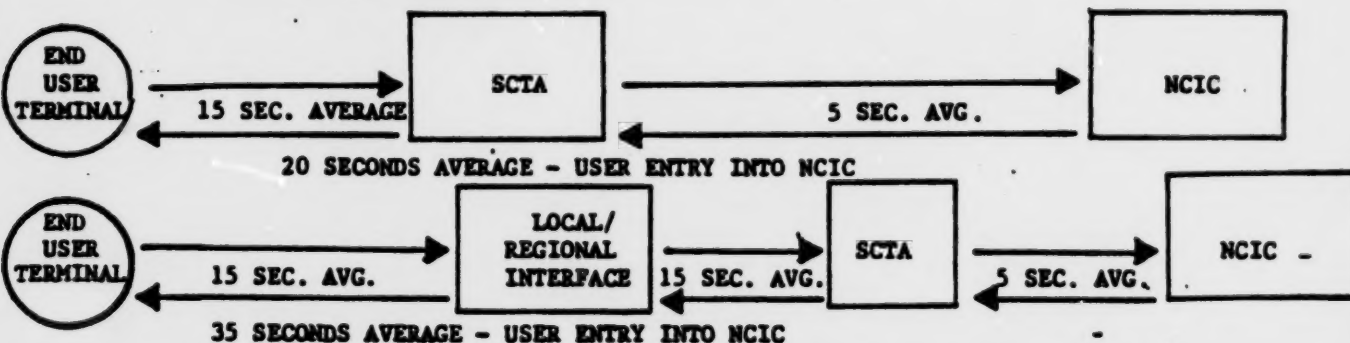
EXAMPLE A: NCIC INQUIRIES - HOT FILES
HIGH SPEED LINES - COMPUTER INTERFACES



EXAMPLE B: NCIC INQUIRIES - III
HIGH SPEED LINES - COMPUTER INTERFACES



EXAMPLE C: NCIC RECORD ENTRY
HIGH SPEED LINES - COMPUTER INTERFACES



NOTE: Times shown above should be considered maximum. In many cases, time will be less depending on individual computer systems being used. All times should be considered on an average when all systems are operating normally. Average time should be based upon a compilation over a one-month period.

STANDARDS FOR AGENCIES RECEIVING A POSITIVE RESPONSE (HIT)

1. Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any of the following actions based upon the hit NCIC record: (1) arresting the wanted person; (2) detaining the missing person; or (3) seizing the stolen property.

Confirming a hit means to contact the agency that entered the record to:

- A. Ensure that the person or property inquired upon is identical to the person or property identified in the record;
 - B. Ensure that the warrant, missing person report, or theft report is still outstanding; and,
 - C. Obtain a decision regarding (1) the extradition of a wanted person, (2) information regarding the return of the missing person to the appropriate authorities, or (3) information regarding the return of stolen property to its rightful owner.
2. Every agency upon taking a person into custody or acquiring property, after confirming the hit, must place a locate on the corresponding NCIC record(s).

STANDARDS FOR SYSTEM AVAILABILITY

The NCIC Computer availability goals shall be 100% with 99% as minimum acceptable performance.

The SCTA computer availability goals shall be 100% with 96% as minimum acceptable performance.

The local/regional computer availability goals shall be 100% with 96% as minimum acceptable performance.

STANDARD REGARDING EQUIPMENT AND TECHNOLOGY COMPATIBILITY

Equipment and/or technological incompatibility shall not be sufficient justification for any agency to operate outside of the normal SCTA configuration.

STANDARDS FOR SERVICES AVAILABILITY

Those services provided by NCIC to the SCTAs shall be provided by the SCTAs to their users with the exception of:

- (1) Services specifically limited to SCTAs by NCIC policy; and
- (2) Services which are restricted to certain users by nature of their governmental and/or criminal justice status and the Federal laws and regulations governing access to certain types of NCIC services.
- (3) Services which may be contrary to a state law or executive order.

"Users" include those agencies having a direct telecommunications link with an SCTA, and any regional dispatch center, electronic switcher, satellite computer, or other computer interface, providing a telecommunications link to user agency as well as those agencies who have no telecommunications link but access an SCTA via another user which has a telecommunications link. Any regional dispatch/communication center shall be required by the SCTA to provide the same services to their users as those provided to them by the SCTA.

Services include:

1. Providing users with the capability of communicating with and receiving responses from all current and future NCIC Files.
 - Article
 - Boat
 - Canadian Warrant

- Gun
 - Interstate Identification Index (III) including the NCIC Federal Offenders File and the FBI Automated Identification Division System (AIDS)
 - License Plate
 - Missing Person
 - Securities
 - Unidentified Person
 - U.S. Secret Service Protective
 - Vehicle
 - Wanted Person
 - ZO
2. The capability to enter an NCIC record into all current and future NCIC Files which:
 - A) Meets the NCIC entry criteria for the file involved;
 - B) Contains at least the minimum data required by NCIC for entry and up to the maximum number of identifiers permitted in the record by NCIC; and
 - C) Contains any of the codes or data permitted by NCIC in each of the fields.
 3. Entry of a valid record shall be permitted regardless of the existence of any other record(s) already entered in NCIC by any other agency(s) for the person or property in question.
 4. The capability to add information to, delete information from, and/or change information in a field(s) of an existing NCIC record.
 5. The capability to remove a record from file when a record is determined to be invalid, e.g., the warrant which was the basis for an entry is dismissed, or when the person or property which is the subject of the record is found.
 6. The capability to place a locate against another agency's NCIC record, including records entered by agencies serviced by the same SCTA as well as records entered by agencies serviced by another SCTA.

The use of the above services by any user agency shall be in accordance with the instructions and procedures contained in the NCIC Operating Manual, the codes contained in the NCIC Code Manual, and new enhancements contained in the NCIC Technical and Operational Update, NCIC Newsletter, or any other official notification from FBI NCIC.

SANCTIONS

Purge of an agency's NCIC records and discontinuance of System access for an agency are the two ultimate sanctions available to NCIC management for enforcement of System policy and procedure. This presumes prosecution for law violations would normally be handled at the state level, directed toward an individual rather than toward an agency.

Inflexible procedures for policy enforcement would be a hinderance to good NCIC management. We recommend, instead of rigid enforcement of the established rules, that NCIC in concert with the CTAs, Regional Working Groups, and the Board utilize the sanctions identified below in a reasonable way to gain compliance with System objectives. Usually problems of a serious nature are corrected quickly through telephone conversations among the parties involved. Each case has peculiarities of its own.

These sanctions should be viewed as part of the package of an improved user agreement and proactive quality assurance measures. It is unlikely a notice of caution would ever be sent to the chief executive of a state. Should it become necessary, however, the Board must make it clear now to every CTA and to NCIC that the Board finds such action reasonable and necessary, and supports FBI enforcement of established NCIC policy.

References to CTAs throughout this report include "other agencies with direct NCIC lines" when the inclusion is logical.

Considerations

1. An up-to-date NCIC/CTA user agreement should be on file with the NCIC Section (copy with CTA) and it should include reference to the sanctions that could be imposed for failure to comply.
2. Specific references should include but not be limited to:
 - Failure to react properly to error notices
 - Failure to react properly to hit confirmation requests
 - Failure to locate
 - Failure to complete entries/modifications/removals promptly

- Failure to make complete entries
 - Failure to validate
 - Failure to assure security of equipment and data
 - Failure to provide qualified operators
 - Entry of invalid or nonqualified records
3. A special audit of a CTA should be part of the sanction package.
 4. Flagging records of substandard CTA lines should be an option.
 5. Deadlines should be imposed on compliance with corrective action notices.
 6. Letters to CTAs, rather than being titled "Caution" should be drafted in the framework of a "request to comply" with NCIC Standards. When prolonged failure to comply would result in discontinuance of service, the letter should be explicit in announcing the "probationary" status of the CTA; or in announcing the date probationary status will begin if compliance is not forthcoming before then.
 7. Unless the serious nature of a problem requires immediate discontinuance of service, a letter to the Governor should precede discontinuance of service.

I. NLETS message transmitted by FBI NCIC to control terminal agency for all nonserious errors

A. Redirection of NLETS message by CTA to offending terminal agency. (CTA to maintain copy of these messages for follow up.)

II. Verbal notice from CTA to terminal agency for nonserious error intercepted by CTA

or

Intrastate message to offending terminal agencies for nonserious errors or reports thereof. (Note: record of verbal notices should be retained by CTA for six months.)

III. Letter of request for compliance

A. FBI NCIC to CTA officer regarding:

1. Untimeliness
2. Inaccuracy
3. Incompleteness
4. Unsatisfactory record quality
5. Unsatisfactory validation
6. Misuse of system
7. Notice of probationary status resulting from audit
 - a) 30 days to correct deficiencies
8. Serious Error

B. CTA to terminal agency

1. Untimeliness
2. Inaccuracy
3. Incompleteness

III. Letter of request for compliance - (cont.)

4. Unsatisfactory record quality
5. Unsatisfactory validation
6. Misuse of system
7. Notice of probationary status resulting from audit
 - a) 30 days to correct deficiencies
8. Serious error

IV. Letter of intent to remove from system if deficiency not corrected

A. Board to CTA head

1. Continuous serious error trend
2. Audit failure status (not corrected within 30 days of first letter of request)
3. Intentional misuse of "PUR/C" Code in III

B. CTA to terminal agency

1. Continuous serious error trend
2. Audit failure status (not corrected within 30 days of first letter of request)
3. Intentional misuse of "PUR/C" Code in III

V. Advisory letter to governor

A. FBI NCIC to governor with copy to CTA

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probationary status has been modified to failure status (additional 30 days to correct)
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

B. CTA to terminal agency - removal of records and discontinuance of service is imminent

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probation status to failure status
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

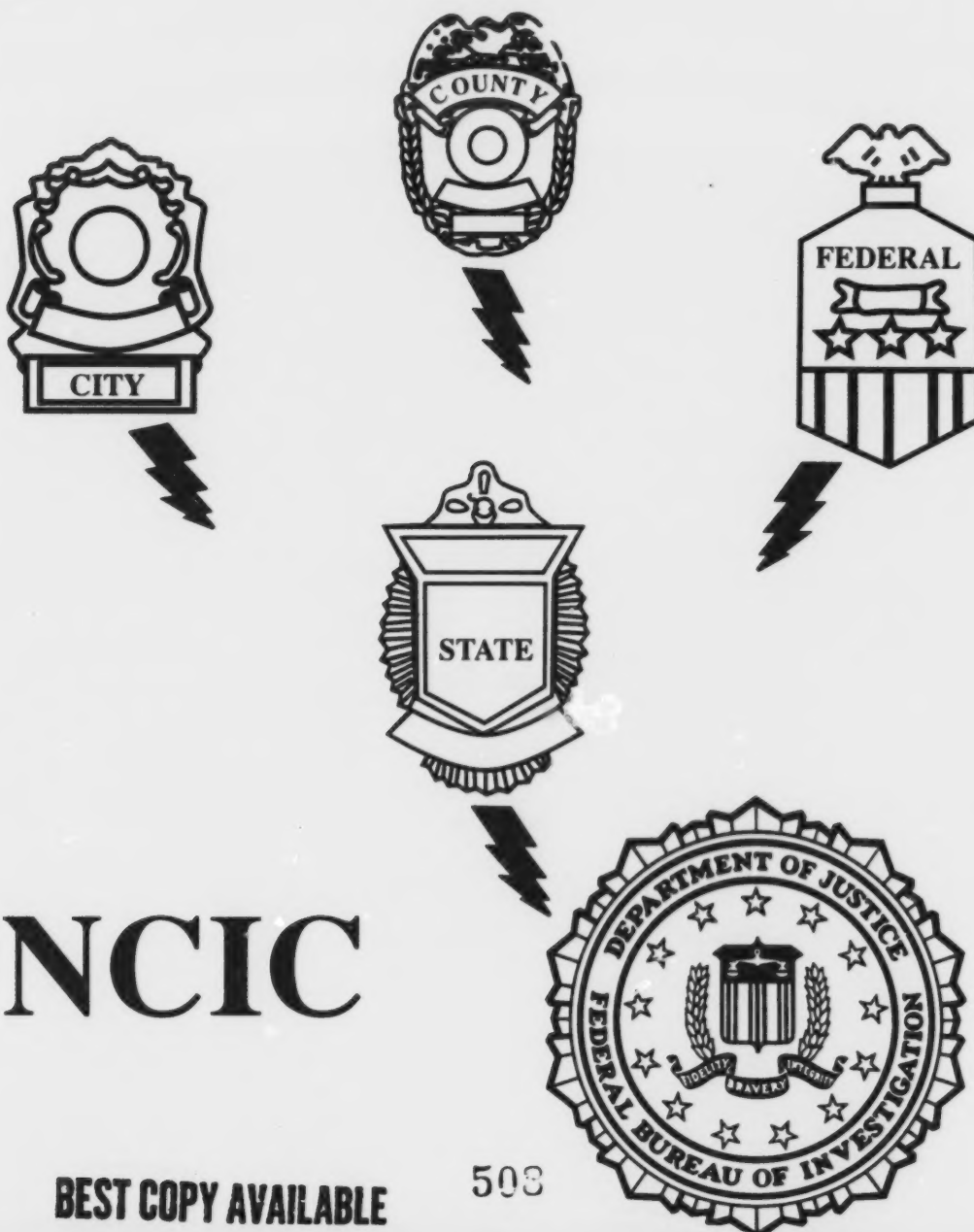
VI. Removal from system includes purge of all records and discontinuance of service pending reinstatement

- A. Board and FBI NCIC jointly initiate removal of CTA/state from active system use
- B. CTA may discontinue service to an offending agency, and purge that agency's records from state and NCIC files

VII. Reinstatement

- A. Upon satisfactory proof the offending state has corrected its deficiencies the Board may reinstate
- B. Upon satisfactory proof offending terminal has corrected its deficiencies CTA may reinstate. CTA also has option to defer to another agency who would become the CTA

**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**



**NATIONAL CRIME INFORMATION CENTER
MANDATORY MINIMUM STANDARDS CURRICULUM
FOR
FULL ACCESS TERMINAL OPERATORS**

LESSON PLAN: INTERSTATE IDENTIFICATION INDEX (III)

TITLE OF INSTRUCTION:

INTERSTATE IDENTIFICATION
INDEX

TIME ALLOTTED:

2 HOURS

TARGET GROUP:

FULL ACCESS TERMINAL
OPERATORS

INSTRUCTOR:

METHOD OF INSTRUCTION:

LECTURE, OVERHEAD
TRANSPARENCIES, AND
VIDEO TAPE PRESENTATION

DATE:

NCIC INTERSTATE IDENTIFICATION INDEX (III) LESSON PLAN
TABLE OF CONTENTS

	PAGE
STATEMENT OF GOAL AND OBJECTIVES	III-1
CRITERION TEST	III-2
CRITERION TEST ANSWERS	III-4
ITEMS AND MATERIALS	III-8
INTRODUCTION	III-9
RECORDS AVAILABLE THROUGH III	III-11
Obtaining Criminal History Records Available Through III	III-11
QH Inquiry	III-11
QR Record Request	III-12
RECORDS NOT AVAILABLE THROUGH III	III-13
III No Record Response	III-13
STATE PARTICIPATION IN III	III-15
Participating States	III-15
Nonparticipating States	III-15
Services Provided By the FBI Identification Division . .	III-15
Multistate Offenders	III-16
Single State Offenders	III-16
RETENTION OF III INDEX RECORDS	III-17
Removal of III Index Records	III-17
III POLICY ISSUES	III-18
Personnel Security	III-18
Physical Security	III-18
Technical Security	III-18
Use and Dissemination	III-19
III Purpose Codes	III-19
III QH INQUIRY	III-22
Purpose	III-22
Requirements	III-22
Interpreting Responses	III-23
Guidelines	III-24
III QR RECORD REQUEST	III-26
Purpose	III-26
Requirements	III-26
Interpreting Responses	III-26
Guidelines	III-28

III ZR INQUIRY	III-30
Purpose	III-30
Requirements	III-30
Interpreting Responses	III-30
Guidelines	III-31
III ZI AND ZRS INQUIRIES	III-32
CONCLUSION	III-33
BIBLIOGRAPHY	III-34

STATEMENT OF GOAL AND OBJECTIVES

INSTRUCTIONAL GOAL:

To provide the terminal operator critical information on the policies, criteria, and transactions for the Interstate Identification Index (III).

INSTRUCTIONAL OBJECTIVES:

At the conclusion of this block of instruction, the operator will be able to:

1. State what criminal history records are available through III.
2. Describe the two transactions by which III provides criminal history records.
3. Explain why a "no record" response for a III inquiry does not necessarily mean there is no criminal history record on a subject.
4. State the definition of participating and nonparticipating states.
5. State the retention period for III Index Records.
6. List, with reference to the NCIC Operating Manual and III Operational and Technical Manual, the personnel, physical, technical, and use and dissemination policies that must be followed by agencies accessing III.
7. State the purpose of a III QH inquiry, QR record request, and ZR inquiry.
8. List the requirements for a III QH inquiry, QR record request, and ZR inquiry.
9. Describe the responses that may be received in a III QH inquiry, QR record request, and ZR inquiry.
10. Describe, with reference to the NCIC Operating Manual and III Operational and Technical Manual, the guidelines that may affect a III QH inquiry, QR record request, and ZR inquiry.

CRITERION TEST

RECORDS AVAILABLE THROUGH III

1. State what criminal history records are available through III.
2. Describe the information that may be obtained through a III QH inquiry.
3. Describe the information that may be obtained through a III QR record request.

RECORDS NOT AVAILABLE THROUGH III

4. III will contain records for juvenile offenders tried as juveniles.
A. True
B. False
5. Explain why a "no record" response for a III inquiry does not necessarily mean there is no criminal history record on the subject.

STATE PARTICIPATION IN III

6. The FBI Identification Division maintains and provides criminal history records for QR record requests for participating states.
A. True
B. False
7. Define a nonparticipating state.
8. The _____ enters all III Index Records.

RETENTION OF III INDEX RECORDS

9. State when a III Index Record is removed.

III POLICY ISSUES

10. List the III physical security policies that must be followed by agencies accessing III.

11. List and describe, with reference to the NCIC Operating Manual and III Operations and Technical Manual, each III purpose code.
12. The Attention Field is mandatory for III QH inquiries.
 - A. True
 - B. False

III QH INQUIRY

13. State the purpose of a III QH inquiry.
14. A QH multiple positive response will provide up to ____ records.
15. The FBI or SID should not be used in QH inquiries.
 - A. True
 - B. False

III QR RECORD REQUEST

16. State the purpose of a QR record request.
17. State the responses that will be received if III is unable to contact the state computer system holding the criminal history record.
18. State how an inquiring agency may receive clarification on a participating state's criminal history record.

III ZR INQUIRY

19. A III ZR inquiry can be made using the ____ or ____.
20. If a purpose code is used in ZR inquiries, it must be either ____ or ____.

CRITERION TEST ANSWERS

RECORDS AVAILABLE THROUGH III

1. The records contained in III are limited to offenders of serious and or significant violations that are:
 - a. known to the FBI.
 - b. with a date of birth of 1956 or later.
 - or
 - c. arrested for the first time and reported to the FBI Identification Division since July 1, 1974 (regardless of date of birth).

Additionally, III will contain selected older records converted to the automated system for certain fugitives and repeat offenders.

2. The QH inquiry is used to obtain the III Index Record. The III Index Record contains four types of information:
 - a. The subject's name(s), physical descriptors, and numeric identifiers (e.g., Date of Birth, Social Security Number).
 - b. The FBI or SID number to be used in the OR record request.
 - c. "Pointers" (FBI or SID) to the database(s) maintaining the criminal history record(s).
 - d. The means to obtain the criminal history record(s) (e.g., NCIC).
3. A QR record request is used to obtain the actual criminal history record(s) from the database maintaining the record(s). A criminal history record contains the following information:
 - a. The subject's name, physical descriptors, and numeric identifiers.
 - b. Arrest, conviction, and sentencing information.

RECORDS NOT AVAILABLE THROUGH III

4. False. III will not contain records for juvenile offenders tried as juveniles.
5. Approximately 15 million of the 23 million fingerprints cards maintained by the FBI Identification Division are indexed in III. The inquiring agency should be aware that a

III no record response does not necessarily mean that there is no criminal history record on the subject.

STATE PARTICIPATION IN III

6. False. Participating states are states that maintain criminal history records and provide QR record responses from its state criminal history files.
7. Nonparticipating states are states where the FBI Identification Division maintains criminal history records and provides responses to QR record requests. The FBI Number (FBI) is listed as the pointer in the index record.
8. The FBI Identification Division enters all III Index Records.

RETENTION OF III INDEX RECORDS

9. An index record remains in III until it is removed due to:
 - a. the subject reaching the age of 80.
 - b. official notification by fingerprint cards of the subject's death.
 - c. the consolidation of the record with another III record when the subject has two or more FBI numbers.
 - d. court-ordered expungement.

III POLICY ISSUES

10. The III physical security policies that must be followed by agencies accessing III are:
 - a. "All agencies having terminals on the system must be required to physically place these terminals in secure locations within the authorized agency." (NCIC OM 10-20, Para VII, (C-1) (11-17-86)
 - b. "It is incumbent upon an agency operating an NCIC terminal to implement the necessary procedures to make that terminal secure from any unauthorized use." (NCIC OM, Intro-5, Para 1.6) (11-17-86)
 - c. "Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data." (NCIC OM, 10-20, Para VII (C-3) (11-17-86)

11. The III purpose codes are:

- a. Criminal Justice (Purpose Code "C") - must be used when the III transaction is for official duties in connection with the administration of criminal justice. (III OTM, 1-2) (7-1-91)
- b. Criminal Justice Employment (Purpose Code "J") - must be used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. (III OTM 1-2) (7-1-91)
- c. Interstate-approved Noncriminal Justice (Purpose Code "I") - must be used when the III transaction involves noncriminal justice employment and/or licensing. Use of purpose code I is limited to one agency in each state with approved state statutes. (III OTM 1-2) (7-1-91)
INSTRUCTOR'S NOTE: PURPOSE CODE "I" IS RESTRICTED TO STATE IDENTIFICATION BUREAUS WHO HAVE BEEN AUTHORIZED BY NCIC.
- d. National Security (Purpose Code "S") - must be used when the III transaction is generated by an agency authorized by the Security Clearance Information Act (SCIA) when investigating individuals for access to classified information or assignment to or retention in sensitive national security duties. Only those agencies having an ORI containing an "R" in the ninth position are authorized to use this purpose code. These agencies are the Department of Defense (DOD), including the Defense Investigative Service (DIS), the U.S. Office of Personnel Management (OPM), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Department of State (DOS). (III OTM, 1-2, 1-3) (7-1-91)
- e. Administrative File Maintenance (Purpose Code "A") - must be used when the authorized participating state agency generates a III transaction for internal review. Responses to transactions containing purpose code A cannot be disseminated for any other purposes. (III OTM, 1-3) (7-1-91)

12. True. The Attention Field is mandatory for III QH inquiries.

III QH INQUIRY

7/1/92

III-6

13. The purpose of a III QH inquiry is to determine if an index record to a subject's criminal history record is maintained in III.
14. A QH multiple positive response will provide up to 15 records.
15. False. The FBI or SID should be used in the QH inquiry if known, as this will provide an exact hit and thus eliminate the possibility of multiple responses.

III QR RECORD REQUEST

16. The purpose of a QR record request is to obtain a specific criminal history record available through III.
17. H-Type Response - indicates to the inquiring agency that III is unable to contact the state computer system maintaining the criminal history record either because the state system is out of service or otherwise unable to accept the request and that III will continue to contact the state computer system for four hours.
or
P-Type Response - indicates to the inquiring agency that the inquiry submitted in which the inquiring agency received a previous H-Type Response has been queued for four hours and has been unsuccessful in contacting the state and that the inquiring agency must resubmit at a later time.
18. Should an inquiring agency receive a state criminal history record that needs clarification, the state criminal history HELP File (SIR) is available through NLETS. The file provides information regarding a state contact person available to answer questions regarding the state's record.

III ZR INQUIRY

19. A III ZR inquiry can be made using the FBI or SID.
20. If a purpose code is used in ZR inquiries, it must be either a "C" or "J".

ITEMS AND MATERIALS

Overhead Projector and Screen

Overhead Transparencies:

- III-OH #1 - Interstate Identification Index
- III-OH #2 - Purpose of III
- III-OH #3 - The Number of Records Available Through III
- III-OH #4 - Criminal History Records Available Through III
- III-OH #5 - The Two Transactions for Obtaining Records Available Through III
- III-OH #6 - III No Record Response
- III-OH #7 - Retention of III Records
- III-OH #8 - III Purpose Codes
- III-OH #9 - III Misuse Warnings
- III-OH #10 - Positive Identification Only by Fingerprint Comparison
- III-OH #11 - Course Summary

Handouts:

- III-HD #1 - Participants Map
- III-HD #2 - SCIA Act
- III-HD #3 - QH Responses
- III-HD #4 - QR Responses
- III-HD #5 - ZR Responses
- III-HD #6 - III Summary Card

VCR and monitor

Video:

III
System Security

I. INTRODUCTION

The Interstate Identification Index (III) was developed in 1978 to coordinate the decentralized exchange of interstate criminal history record information among states and Federal criminal justice agencies to contend with interstate criminal mobility.

Among the many benefits III provides are:

1. a national index; authorized users need only make one inquiry instead of multiple inquiries to each state,
2. a backup for state files in case of state disaster,
3. standardization of criminal history record information through NCIC formats and fields,
4. a response in minutes for over 16 million criminal history records.

The purpose of III is to coordinate the exchange of criminal history record information; not to replace state criminal history files. State criminal history systems are essential because:

1. 66% of criminal history records are single state offenders, i.e. subject commits crime in one state only,
2. state criminal history systems can best satisfy state, local, or special criminal history record information needs,
3. a state criminal history system adheres to the NCIC shared management concept.
4. a state criminal history system has the resources to contain misdemeanors and other crimes that would not warrant entry into III.

References

IO =
Instructional
Objectives

OH =
Overhead
Transparencies

HO =
Handouts

OH #1

NCIC OM =
NCIC Operating
Manual

III OTM
III Operational
and Technical
Manual

OH #2

The FBI Identification Division is responsible for the maintenance of III. As of January 1, 1992, there were 15,273,539 records in the III System. Approximately 89,000 records are added to III each month.

OH #3

The information presented in this lesson plan is important as it provides guidelines for the proper use of III. Effective utilization of III will enhance criminal justice operations, help reduce liability, and create a safer environment for the criminal justice community.

II. RECORDS AVAILABLE THROUGH III

IO #1

The records contained in III are limited to offenders of serious and or significant violations that are:

OH #4

1. known to the FBI,
2. with a date of birth of 1956 or later,
- or
3. arrested for the first time and reported to the FBI Identification Division since July 1, 1974 (regardless of date of birth),

Additionally, III will contain selected older records converted to the automated system for certain fugitives and repeat offenders.

A. Obtaining Criminal History Records Available Through III

IO #2

III provides criminal history records through two transactions: the QH inquiry and the QR record request.

OH #5

1. The QH inquiry is used to obtain the III Index Record. The III Index Record contains four types of information:
 - a. The subject's name(s), physical descriptors, and numeric identifiers (e.g., Date of Birth, Social Security Number),
 - b. The FBI or SID number to be used in the QR record request,
 - c. "Pointers" (FBI or SID) to the database(s) maintaining the criminal history record(s),
 - d. The means to obtain the criminal history record(s) (e.g., NCIC).

2. A QR record request is used to obtain the criminal history record(s) from the database maintaining the record(s). A criminal history record contains the following information:

- a. the subject's name, physical descriptors, and numeric identifiers,
- b. arrest, conviction, and sentencing information.

INSTRUCTOR'S NOTE: FOR SPECIFIC INFORMATION REGARDING THE QH INQUIRY AND QR RECORD REQUEST, SEE PART VI. III QH INQUIRY (PAGE 23) AND PART VII. III QR RECORD REQUEST (PAGE 27).

III. RECORDS NOT AVAILABLE THROUGH III

III does not contain the following records:

1. subjects not meeting age criteria and arrest criteria,
2. subjects who have been arrested but whose fingerprint cards were not received by the FBI Identification Division,
3. juvenile offenders tried as juveniles,
4. charges of drunkenness and vagrancy,
5. certain public order offenses, e.g. disturbing the peace, curfew violations, loitering, false fire alarms, traffic violations (except driving under the influence, driving while intoxicated, manslaughter),
6. nonspecific charges of suspicion or investigation,
7. social history data, e.g. narcotic, civil commitment, or mental hygiene - unless part of the criminal justice process.

A. III No Record Response

Approximately 16 million of the 23 million fingerprint cards maintained by the FBI Identification are indexed in III. The inquiring agency should be aware that a III no record response does not necessarily mean that there is no criminal history record on the subject.

If a no record response to a III inquiry is received, the inquiring agency should either request a manual name search or

IO #3

OH #6

submit a fingerprint card containing the subject's fingerprints to the FBI Identification Division. An agency should also make inquiries, via the National Law Enforcement Telecommunications Network System (NLETS), to any state systems where it is suspected an individual may have a record.

INSTRUCTOR'S NOTE: FOR MORE INFORMATION REFER TO THE NLETS MANUAL OR CONSULT YOUR CONTROL TERMINAL AGENCY.

IV. STATE PARTICIPATION IN III

III is a national index of state and Federal criminal history records. The extent of a state's participation in III is determined by the state's status as a Participating or Nonparticipating State:

1. Participating States - Participating states are states that maintain criminal history records and provide QR record responses from its state criminal history files. The participating state's SID is listed as a pointer in the index record. Currently 22 states provide approximately one half of the criminal history records available through III. This represents nearly 80% of all criminal fingerprints received by the FBI Identification Division.
2. Nonparticipating States - Nonparticipating states are states where the FBI Identification Division maintains criminal history records and provides responses to QR record requests. The FBI is listed as the pointer in the index record. The FBI Identification Division provides records for Federal offenders and the 28 states not capable of providing their own criminal history records.
INSTRUCTOR'S NOTE: THE FBI IDENTIFICATION DIVISION MAINTAINS CRIMINAL HISTORY RECORDS AND PROVIDES RESPONSES FOR THE DISTRICT OF COLUMBIA, PUERTO RICO, AND OTHER FOREIGN COUNTRIES.

The FBI Identification Division also provides the following services:

1. The FBI Identification Division enters index records for both participating and nonparticipating states. The record entry is based on the subject's fingerprint card received at the FBI Identification Division. The FBI Identification Division also provides responses to all QH inquiries for index records.

2. The FBI Identification Division, upon request, will enter or delete data from multistate offender index records.

INSTRUCTOR'S NOTE: MULTISTATE OFFENDER RECORDS ARE WHERE THE SUBJECT HAS BEEN ARRESTED BY MORE THAN ONE STATE OR FEDERAL AGENCY.

INSTRUCTOR'S NOTE: PARTICIPATING STATES HAVE THE CAPABILITY TO ENTER AND DELETE INFORMATION FROM SINGLE STATE OFFENDER RECORDS BASED ON THE FINGERPRINT CARD.

INSTRUCTOR'S NOTE: A SINGLE STATE OFFENDER RECORD IS WHERE THE SUBJECT HAS BEEN ARRESTED BY ONE STATE OR HAS ONE OR MORE FEDERAL ARRESTS. CONSULT YOUR STATE IDENTIFICATION BUREAU FOR MORE INFORMATION.

3. The FBI Identification Division provides participating states arrest information and updates for their criminal history records. When a person is arrested for the first time in a participating state and the subject's record is available through III, that state will be advised by the FBI Identification Division if the subject is a single state or a multistate offender.

If the status of a single state offender changes to multistate offender, the participating state(s) will be notified by III. This information is determined by fingerprint cards submitted to the FBI Identification Division.

4. The FBI Identification Division receives the QR record requests for participating states, acknowledges the QR record request to the inquiring agency, and forwards the QR record request onto the appropriate participating state(s). (QR record responses are covered in Part VII. III QR Record Request.)

INSTRUCTOR'S NOTE: CONSULT YOUR STATE IDENTIFICATION BUREAU FOR MORE SPECIFIC INFORMATION REGARDING TOPICS COVERED IN THIS SECTION.

V. RETENTION OF III INDEX RECORDS

A. Retention of III Index Records

IO #5

An index record remains in III until it is removed due to:

OH #7

1. the subject reaching the age of 80,
2. official notification by fingerprint cards of the subject's death,
3. the consolidation of the record with another III record when the subject has two or more FBI numbers,
4. court-ordered expungement.

B. Removal of III Index Records

The FBI Identification Division is responsible for consolidating all index records and for purging a III Index Record when the subject reaches the age of 80.

INSTRUCTOR'S NOTE: AN III INQUIRY MADE ON A PERSON OVER THE 80 YEARS OLD WILL RESULT IN A REJECT OF "FIELD ERROR DATE OF BIRTH."

The FBI Identification Division is also responsible for removing index records for nonparticipating states and Federal agencies due to official notification of the subject's death by fingerprint cards or court-ordered expungement.

Participating states are responsible for removing their index records when the state receives official notification by fingerprint cards of a subject's death or court-ordered expungement.

V. III POLICY ISSUES

Each criminal justice agency authorized to receive III must sign a written agreement with its Control Terminal Agency (CTA) or Service Coordinator (SC). This agreement states that the criminal justice agency will conform to the following policies designed to ensure the authorized use, access, and dissemination of III information:

IO #6

A. Personnel Security

1. "The agencies having terminals with access to criminal history must have terminal operators screened and restrict access to the terminal to a minimum number of authorized employees." (NCIC OM 10-20, Para VII (C-2) (11-17-86))

B. Physical Security

1. "All agencies having terminals on the system must be required to physically place these terminals in secure locations within the authorized agency." (NCIC OM 10-20, Para VII, (C-1) (11-17-86))
2. "It is incumbent upon an agency operating an NCIC terminal to implement the necessary procedures to make that terminal secure from any unauthorized use." (NCIC OM, Intro-5, Para 1.6) (11-17-86)
3. "Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data." (NCIC OM, 10-20, Para VII (C-3) (11-17-86))

C. Technical Security

1. "That by no later than December 31, 1985, each State Control Terminal (SCTA) and Service Coordinator (SC) have in place at the SCTA or SC level an automated System

for logging all inquiries of the Interstate Identification Index (III), which log shall include the name of the individual within the criminal justice agency to whom the response is given. These logs shall be maintained for at least 12 months from the date of inquiry." (Advisory Policy Board Minutes, Page 310) (10-84)

INSTRUCTOR'S NOTE: THIS POLICY INCLUDES THE AUTOMATED LOGGING BY THE CTA OF ALL QH INQUIRIES.

D. Use and Dissemination

1. "Due to variance in state laws and policies, the III cannot be used for licensing or noncriminal justice employment purposes." (NCIC OM, 10-25, Para 3.1) (11-1-87)
2. "The III shall not be used for remote access to a record to be reviewed and or challenged by the subject of the record. Record requests for this purpose must be submitted in writing either to the FBI Identification Division or state of record." (III OTM, Intro-6) (7-1-91)
3. "Inquiries and record requests transmitted to the III must include the purpose for which the information is to be used.
 - a. Criminal Justice (Purpose Code "C") - must be used when the III transaction is for official duties in connection with the administration of criminal justice. (III OTM, 1-2) (7-1-91)
INSTRUCTOR'S NOTE: SOME STATES ALLOW III TO BE UTILIZED FOR FIREARM PERMIT APPLICATIONS. CONSULT YOUR CONTROL TERMINAL AGENCY FOR MORE INFORMATION.
 - b. Criminal Justice Employment (Purpose Code "J") - must be used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control. Criminal justice

OH #8

employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. (III OTM 1-2) (7-1-91)

- c. Interstate-approved Noncriminal Justice (Purpose Code "I") - must be used when the III transaction involves noncriminal justice employment and/or licensing. Use of purpose code I is limited to one agency in each state with approved state statutes. (III OTM 1-2) (7-1-91)

INSTRUCTOR'S NOTE: PURPOSE CODE "I" IS RESTRICTED TO STATE IDENTIFICATION BUREAUS THAT ARE AUTHORIZED BY NCIC.

- d. National Security (Purpose Code "S") - must be used when the III transaction is generated by an agency authorized by the Security Clearance Information Act (SCIA) when investigating individuals for access to classified information or assignment to or retention in sensitive national security duties. Only those agencies having an ORI containing an "R" in the ninth position are authorized to use this purpose code. These agencies are the Department of Defense (DOD), including the Defense Investigative Service (DIS), the U.S. Office of Personnel Management (OPM), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Department of State (DOS). (III OTM, 1-2, 1-3) (7-1-91)

HD #2

- e. Administrative File Maintenance (Purpose Code "A") - must be used when the authorized participating state agency generates a III transaction for internal review. Responses to transactions containing purpose code A cannot be disseminated for any other purposes. (III OTM, 1-3) (7-1-91)"

INSTRUCTOR'S NOTE: STRESS TO THE STUDENTS THAT THESE ARE THE ONLY PURPOSES FOR WHICH III CAN BE USED. OBTAINING III FOR ANY OTHER PURPOSE CONSTITUTES MISUSE. BOTH

OH #9

ADMINISTRATIVE AND CRIMINAL SANCTIONS CAN
BE TAKEN AGAINST AGENCIES AND INDIVIDUALS
THAT MISUSE III.

4. "Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the transmission of criminal history beyond that information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public. When an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public, then details of criminal history record information may be transmitted. (NCIC OM, 10-20, Para VII)(B-3)
5. "Each criminal justice agency receiving an III response shall record any secondary dissemination of any III response to another criminal justice agency or an individual within another criminal justice agency, or to anyone legally entitled to receive such information who is outside the original receiving agency. These logs shall be maintained for at least 12 months. (Advisory Policy Board Minutes, Page 310)(10-84)

INSTRUCTOR'S NOTE: A FACSIMILE MACHINE MAY BE USED TO TRANSMIT III INFORMATION PROVIDED THAT BOTH AGENCIES INVOLVED HAVE AN ORIGINATING AGENCY IDENTIFIER (ORI) AUTHORIZED TO RECEIVE CRIMINAL HISTORY INFORMATION. AS NOT ALL FACSIMILE MACHINES ARE MONITORED CONTINUALLY, THE RECEIVING AGENCY SHOULD BE NOTIFIED PRIOR TO TRANSMITTING THE INFORMATION. THIS WILL ENSURE PROPER RETRIEVAL OF INFORMATION.

INSTRUCTOR'S NOTE: MANY STATE AND LOCAL SYSTEMS HAVE ADDITIONAL REGULATIONS CONCERNING THE USE OF CRIMINAL HISTORY FILES. CONSULT YOUR STATE CONTROL TERMINAL AGENCY AND STATE SYSTEM OPERATING MANUAL FOR MORE INFORMATION.

VI. III QH INQUIRY

A. Purpose

IO #7

The purpose of a III QH inquiry is to determine if an index record to a subject's criminal history record is maintained in III.

Inquiries should be made on, but not limited to:

1. investigative purposes on fugitives,
2. screening applications for firearms-related permits but only when a Federal, state, or local law exists making the criminal justice agency responsible for the issuance of the license/permits,
3. protective services pertaining to the physical protection of authorized persons (dignitaries) both foreign and domestic,
4. security of criminal justice facilities to include screening visitors, vendor's access to the prison, mail lists, classification and assignment of prisoners,
5. matters involving a violation of U.S. immigration laws including both criminal matters that can lead to criminal charges and administrative action that can lead to deportation,
6. employment in criminal justice agencies and over agencies where a criminal justice agency has management control.

B. Requirements

IO #8

To make a QH inquiry, the Message Key (MKE), Originating Agency Identifier (ORI), Purpose Code (PUR) and Attention Field (ATN) must be used in addition to the following fields:

1. Name (NAM), Sex, Race (RAC), and Date of Birth (DOB),
or
2. NAM, Sex, RAC, DOB, Social Security Number (SOC),
or
3. NAM, Sex, RAC, DOB, Miscellaneous Number (MNU),

- or
- 4. NAM, SOC,
- or
- 5. NAM, MNU,
- or
- 6. State Assigned Number (SID),
- or
- 7. NAM, SID,
- or
- 8. FBI,
- or
- 9. NAM, FBI,

C. Interpreting Responses

IO #9

An III QH inquiry will cause the NCIC computer to transmit the following responses:

HD #3

1. Single Positive Response - indicates to the inquiring agency that the descriptors in the inquiry match descriptors in a single NCIC III Index Record.
or
2. Multiple Positive Response - indicates to the inquiring agency that the descriptors in the inquiry match descriptors in multiple NCIC III Index Records. Up to 15 records will be furnished in response.
INSTRUCTOR'S NOTE: ONLY THE FBI NUMBERS OF ANY ADDITIONAL MATCHING RECORDS WILL BE PROVIDED AFTER THE 15TH MULTIPLE RESPONSE.
or
3. Response When the Index Record Has Been Removed From III as a Result of Consolidation, Deletion, Expungement, or Subject's Death - indicates to the inquiring agency that the record is no longer available.
or
4. G-Type Response - indicates to the inquiring agency that the NCIC III QH inquiry response cannot be provided automatically due to technical problems. If the response is not provided after three hours, the QH inquiry will be purged. The inquiring agency is notified of the purge by another G-Type Response. The inquiring agency may resubmit the inquiry at a later time.

5. No Response - indicates to the inquiring agency that the descriptors in the inquiry do not match descriptors in any NCIC III Index Record.
or
6. Reject - indicates to the inquiring agency that the inquiry was unsuccessful due to an error in either the data, codes, or format of the NCIC QH inquiry.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA AND ANY LOCAL SYSTEMS FOR MORE INFORMATION REGARDING NCIC III RESPONSES. YOUR SYSTEM MAY USE DIFFERENT TERMINOLOGY. THE SEARCH CRITERIA OF YOUR STATE SYSTEM MAY ALSO AFFECT RESPONSES.

D. Guidelines

IO #10

1. Care should be taken when interpreting records as the QH inquiry response may contain multiple subjects. A positive identification can only be made by comparison of fingerprints.
2. The III QH inquiry response should be used as a table of contents to be attached on top of any criminal history records received later. This will allow the requestor to know when all the possible responses are received.
3. The FBI or SID should be used in the QH inquiry if known, as this will provide an exact hit and thus eliminate the possibility of multiple responses.
4. QH inquiries should contain a last name, first name, and middle name or initial as an inquiry containing only last name and first initial may result in multiple responses.
5. If a subject has a single name as his/her entire name, the single name should be entered as the last name, followed by XXX as the first name, e.g., NAM/Harrison, XXX.
6. Names in III are computer coded or "read" according to a phonetic technique that generally treats all vowels equally and eliminates double consonants. (See NCIC OM, 10-38)

QH #10

(11-17-86) for more information).
INSTRUCTOR'S NOTE: PHONETIC SEARCHING
DOES NOT APPLY TO THE NCIC WANTED PERSON
FILE WHICH EMPLOYS A SOUNDINDEXING SEARCH
TECHNIQUE (REFER TO THE WANTED PERSON
LESSON PLAN.)

7. When a complete DOB is used in the inquiry, the search will provide records that match the name (according to soundex edits), sex, race, and 1) the complete DOB or 2) the same month and day of birth, plus or minus three years on the year of birth.
8. An inquiry which contains an incomplete DOB will be rejected.
9. QH inquiries containing NAM and SOC, NAM and MNU, NAM and FBI, or NAM and SID will be searched on SOC, MNU, FBI, or SID only.
10. A QH inquiry made by NAM/Doe, John or Doe, Jane and SEX, RAC, and DOB will produce a no record response from III.
11. The index record may provide additional identifiers which may not be included in the criminal history record.
12. A response indicating that the record is no longer available in III due to consolidation, deletion, expungement, or subject's death will be provided only when the inquiry is made with a FBI.
13. A response indicating that a FBI has been deleted does not necessarily mean that the FBI is invalid. There are several circumstances that may require the deletion of a record from III even though the record is still available from the FBI Identification Division, e.g., subject turned 80 years old. To determine if a record exists, users should contact III at 202-324-3652.

VII. III QR RECORD REQUEST

A. Purpose

IO #7

The purpose of a QR record request is to obtain a specific criminal history record available through III.

B. Requirements

IO #8

To make a QR record request, the Message Key (MKE), Originating Agency Identifier (ORI), Purpose Code (PUR), and Attention Field (ATN) must be used in addition to the following fields:

1. FBI Number (FBI),
or
2. State Assigned Number (SID).

C. Interpreting Responses

IO #9

An NCIC III QR inquiry will cause the NCIC computer to transmit the following responses:

HD #4

1. F-Type Positive Response - indicates to the inquiring agency that the descriptors in the inquiry match descriptors in a criminal history record maintained by the FBI Identification Division or the FBI Identification Division and a participating state. This response notifies the requestor that 1) the FBI record is being processed and 2) another NCIC response can be expected.
and
2. 4-Type Positive Response - this response is furnished after the F-Type response and contains the criminal history record maintained by the FBI Identification Division.
or
3. E-Type Positive Response - indicates to the inquiring agency that the descriptors in the inquiry match descriptors in an NCIC criminal history record maintained by a participating state. This response notifies the requestor that a response can be expected from the participating state.

- or
4. E-Type Response Indicating that the Inquiring Agency's State Repository Maintains the Only Record on the Subject - indicates to the inquiring agency that the agency's state identification bureau maintains the only criminal history record and that the inquiry must be made to the state repository directly.
- or
5. G-Type Response - indicates to the inquiring agency that the NCIC III QR record request response cannot be provided automatically due to technical problems. If after three hours the response can not be provided, the QR record request will be purged. The inquiring agency is notified of the purge by another G-Type Response. The inquiring agency may resubmit the record request at a later time.
- or
6. H-Type Response - indicates to the inquiring agency that III is unable to contact the state computer system maintaining the criminal history record either because the state system is out of service or otherwise unable to accept the request and that III will continue to contact the state computer system for four hours.
- or
7. P-Type Response - indicates to the inquiring agency that the inquiry submitted in which the inquiring agency received a previous H-Type Response has been queued for four hours and has been unsuccessful in contacting the state and that the inquiring agency must resubmit at a later time.
- or
8. 2-Type Response - indicates to the inquiring agency that the record has been removed from III as a result of consolidation, deletion, expungement, or subject's death.
- or
9. N-Type (No response) - indicates to the inquiring agency that the descriptors in the inquiry do not match descriptors in any criminal history record available through III.
- or

10. J-Type (Reject) - indicates to the inquiring agency that the inquiry was unsuccessful due to an error in either the data, codes, or format of the NCIC QR record request.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA AND ANY LOCAL SYSTEMS FOR MORE INFORMATION REGARDING NCIC III RESPONSES. YOUR SYSTEM MAY USE DIFFERENT TERMINOLOGY. THE SEARCH CRITERIA OF YOUR STATE SYSTEM MAY ALSO AFFECT RESPONSES.

D. Guidelines

IO #10

1. The FBI or SID used in the QR record request may be obtained from a QH inquiry or from other sources available to the inquiring agency, e.g., local investigative files.
2. A model state record format similar to the FBI record has been designed for use by the state systems. States not adopting the model will provide criminal history records in the format already existing for their state systems.
3. Should an inquiring agency receive a state criminal history record that needs clarification, the state criminal history HELP File (SIR) is available through NLETS. The file provides information regarding a state contact person available to answer questions regarding the state's record.

INSTRUCTOR'S NOTE: REFER TO THE NLETS MANUAL FOR MORE INFORMATION.

4. III has single state and multistate test records for each participating state. The FBI of each test record is listed in the NCIC Operating and III manual. The test records should be used for training and testing rather than actual III records.
5. A 2-Type response indicating that the criminal history record has been removed due to consolidation, deletion, expungement, or subject's death will be provided only when the QR record request is made using the FBI.
6. A 2-Type response indicating a FBI has been deleted does not necessarily mean

the FBI is invalid. There are several circumstances that require the deletion of a record from III even though the record may be available from III. To determine if a record exists, users should contact III at 202-324-3652.

7. III does not provide a means for requesting only one criminal history record from a multistate record. Upon receipt of a QR record request, III automatically notifies all databases containing criminal history records on the subject.
8. The NAM is optional with FBI. If the NAM is used with the FBI or SID, it will not be searched by the NCIC computer.

VIII. III ZR INQUIRY

A. Purpose

IO #7

The purpose of a III ZR inquiry is to determine if a record to a FBI Number (FBI) or State Assigned Number (SID) is available through III. This inquiry is used primarily for administrative purposes.

B. Requirements

IO #8

To make a ZR inquiry, the Message Key (MKE), and Originating Agency Identifier (ORI) must be used in addition to the following fields:

1. FBI,
or
2. SID.

C. Interpreting Responses

IO #9

An III ZR inquiry will cause the NCIC computer to transmit one of the following responses:

HD #5

1. Positive Response - indicates to the inquiring agency that the FBI or SID is on file in III.
or
2. No Response Due to Consolidation, Deletion, Expungement, or Subject's Death - indicates to the inquiring agency that the record is no longer available.
or
3. No Response - indicates to the inquiring agency that the FBI or SID is not on file in III.
or
4. Reject - indicates to the inquiring agency that the inquiry was unsuccessful due to an error in either the data, codes, or format of the NCIC ZR inquiry.

INSTRUCTOR'S NOTE: CHECK WITH YOUR CTA AND ANY LOCAL SYSTEMS FOR MORE INFORMATION REGARDING NCIC III RESPONSES. YOUR SYSTEM MAY USE DIFFERENT TERMINOLOGY. THE SEARCH CRITERIA OF YOUR STATE SYSTEM MAY ALSO AFFECT RESPONSES.

D. Guidelines

IO #10

1. The Purpose Code Field is not mandatory for ZR inquiries. If it is used it must be either PUR/"C" or "J". If it is not used, the ZR inquiry is considered to be for administrative purposes.
2. A response indicating that the record is no longer available in III due to consolidation, deletion, expungement, or subject's death will be provided only when the inquiry is made with an FBI.
3. A no record response indicating that a FBI has been deleted does not necessarily mean that the FBI is invalid. There are several circumstances that may require the deletion of a record from III even though the record is still available from III. To determine if a record exists, users should contact III at 202-324-3652.

IX. III ZI AND ZRS INQUIRIES

INSTRUCTOR'S NOTE: INFORM STUDENTS THAT ONLY THE STATE IDENTIFICATION BUREAU IN PARTICIPATING STATES CAN MAKE ZI AND ZRS INQUIRIES. CHECK WITH YOUR STATE CONTROL TERMINAL AGENCY FOR MORE INFORMATION.

X. CONCLUSION

III is extremely successful in coordinating the exchange of criminal history information among states and Federal agencies. III is a key factor in contending with interstate criminal mobility.

In utilizing III, it is particularly important to remember:

1. Obtaining III records usually requires two inquiries: the QH inquiry and the QR record request.
2. The no record response to a III inquiry does not necessarily mean there is no criminal history record for the subject.
3. Administrative and criminal sanctions can be taken against agencies and individuals who use III for any other reason than an official criminal justice purpose.

Effective utilization of the guidelines presented in this lesson plan will help ensure that the correct procedures are followed in the use, access, and dissemination of III information.

INSTRUCTOR'S NOTE: SHOW THE NCIC VIDEOS "III" AND "SYSTEM SECURITY."

OH #11

HD #5

BIBLIOGRAPHY

Federal Bureau of Investigation, Identification Division, Washington, D.C. Interstate Identification Index, Operational and Technical Manual, July 1, 1991 (Participating States' Control Terminal Agencies and Identification Bureaus have a copy of this manual).

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. "Interstate Identification Index (III), A Summary," October 10, 1991.

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. "NCIC III" and "System Security" Video.

Federal Bureau of Investigation, National Crime Information Center, Washington, D.C. National Operating Manual, May 31, 1989. Revision 55.

THE INTERSTATE IDENTIFICATION INDEX (III)

THE PURPOSE OF III

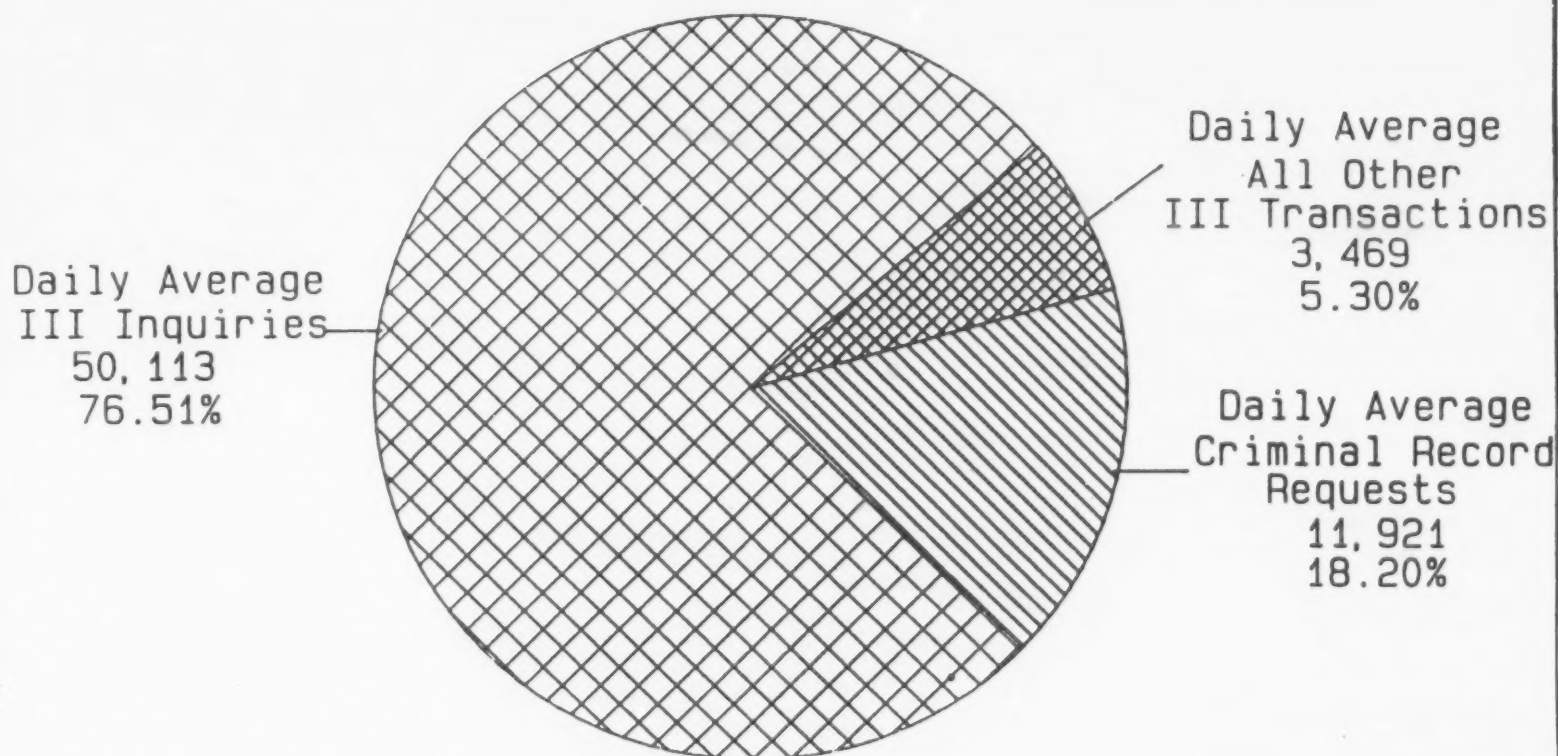
**THE PURPOSE OF III IS TO COORDINATE THE EXCHANGE OF
CRIMINAL HISTORY RECORD INFORMATION; NOT TO REPLACE
STATE CRIMINAL HISTORY FILES.**

INTERSTATE IDENTIFICATION INDEX SUBSYSTEM

15,273,539 Total Records on File on January 1, 1992

2,030,580 Total Transactions in December, 1991

(6.20% of 32,760,409 Total NCIC Transactions)



CRIMINAL HISTORY RECORDS AVAILABLE THROUGH III

**THE RECORDS CONTAINED IN III ARE LIMITED TO
OFFENDERS OF SERIOUS AND OR SIGNIFICANT VIOLATIONS
THAT ARE:**

- 1) KNOWN TO THE FBI,**
- 2) WITH A DATE OF BIRTH OF 1956 OR LATER**
- OR**
- 3) ARRESTED FOR THE FIRST TIME AND REPORTED TO THE
FBI IDENTIFICATION DIVISION SINCE JULY 1, 1974
(REGARDLESS OF DATE OF BIRTH).**

**ADDITIONALLY, III WILL CONTAIN SELECTED OLDER RECORDS
CONVERTED TO THE AUTOMATED SYSTEM FOR CERTAIN
FUGITIVES AND REPEAT OFFENDERS.**

**THE TWO TRANSACTIONS FOR OBTAINING RECORDS AVAILABLE
THROUGH III**

**1. THE QH INQUIRY IS USED TO OBTAIN THE III INDEX
RECORD. THE III INDEX RECORD CONTAINS FOUR TYPES
OF INFORMATION:**

- A. THE SUBJECT'S NAME(S), PHYSICAL DESCRIPTORS,
AND NUMERIC IDENTIFIERS,**
- B. THE FBI OR SID NUMBER TO BE USED IN THE QR
RECORD REQUEST,**
- C. POINTERS TO THE DATABASE(S) MAINTAINING THE
CRIMINAL HISTROY RECORD(S) (e.g. FBI, SID),**
- D. THE MEANS TO OBTAIN THE QR RECORD(S) (e.g., NCIC).**

**2. A QR RECORD REQUEST IS USED TO OBTAIN THE
CRIMINAL HISTORY RECORD(S) FROM THE DATABASE
MAINTAINING THE RECORD(S). A CRIMINAL HISTORY
CONTAINS THE FOLLOWING INFORMATION:**

- A. THE SUBJECT'S NAME, PHYSICAL DESCRIPTORS, AND
NUMERIC IDENTIFIERS,**
- B. ARREST, CONVICTION, AND SENTENCING INFORMATION.**

III NO RECORD RESPONSE

A III NO RECORD RESPONSE DOES NOT NECESSARILY MEAN THAT THERE IS NO CRIMINAL HISTORY RECORD ON THE SUBJECT.

IF A NO RECORD RESPONSE TO A III INQUIRY IS RECEIVED, THE INQUIRING AGENCY SHOULD SUBMIT A FINGERPRINT CARD CONTAINING THE SUBJECT'S FINGERPRINTS TO THE FBI IDENTIFICATION DIVISION. AN AGENCY SHOULD ALSO MAKE INQUIRIES TO ANY STATE SYSTEMS, VIA NLETS WHERE THE INDIVIDUAL MAY HAVE A CRIMINAL RECORD.

RETENTION OF III RECORDS

A III INDEX RECORD REMAINS IN III UNTIL IT IS REMOVED
DUE TO:

1. THE SUBJECT REACHING THE AGE OF 80,
2. OFFICIAL NOTIFICATION OF THE SUBJECT'S DEATH,
3. THE CONSOLIDATION OF THE RECORD WITH ANOTHER
III RECORD WHEN THE SAME SUBJECT HAS TWO OR
MORE FBI NUMBERS,
4. COURT-ORDERED EXPUNGEMENT.

III PURPOSE CODES

- a. Criminal Justice (PURPOSE CODE "C") - Must be used when the III transaction is for official duties in connection with the administration of criminal justice. (III OTM 1-2) (7-1-91)
- b. Criminal Justice Employment (PURPOSE CODE "J") - must be used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. (III OTM 1-2) (7-1-91)
- c. Interstate-approved Noncriminal Justice (PURPOSE CODE "I") - must be used when the III transaction involves noncriminal justice employment and/or licensing. Use of purpose code I limited to one agency in each state with approved state statutes. (III OTM 1-2) (7-1-91)
- d. National Security (PURPOSE CODE "S") - must be used when the III transaction is generated by an agency authorized by the Security Clearance Information Act (SCIA) when investigating individuals for access to classified information or assignment to or retention in sensitive national security duties. Only those agencies having an ORI containing an "R" in the ninth position are authorized to use this purpose code. These agencies are the Department of Defense (DOD), including the Defense Investigative Service (DIS), the U.S. Office of Personnel Management (OPM), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Department of State (DOS). (III OTM, 1-2, 1-3) (7-1-91)
- e. Administrative File Maintenance (PURPOSE CODE "A") - must be used when the authorized participating state agency generates a III transaction for internal review. Responses to transactions containing purpose code A cannot be disseminated for any other purposes. (III OTM, 1-3) (7-1-91)"

III MISUSE WARNINGS

OBTAINING III FOR ANY UNAUTHORIZED PURPOSE
CONSTITUTES MISUSE. BOTH ADMINISTRATIVE AND
CRIMINAL SANCTIONS CAN BE TAKEN AGAINST AGENCIES
AND INDIVIDUALS THAT MISUSE III.

POSITIVE IDENTIFICATION ONLY BY FINGERPRINT COMPARISON

**CARE SHOULD BE TAKEN WHEN INTERPRETING RECORDS AS
THE QH RESPONSE MAY CONTAIN MULTIPLE SUBJECTS. A
POSITIVE IDENTIFICATION CAN ONLY BE MADE BY
COMPARISON OF FINGERPRINTS.**

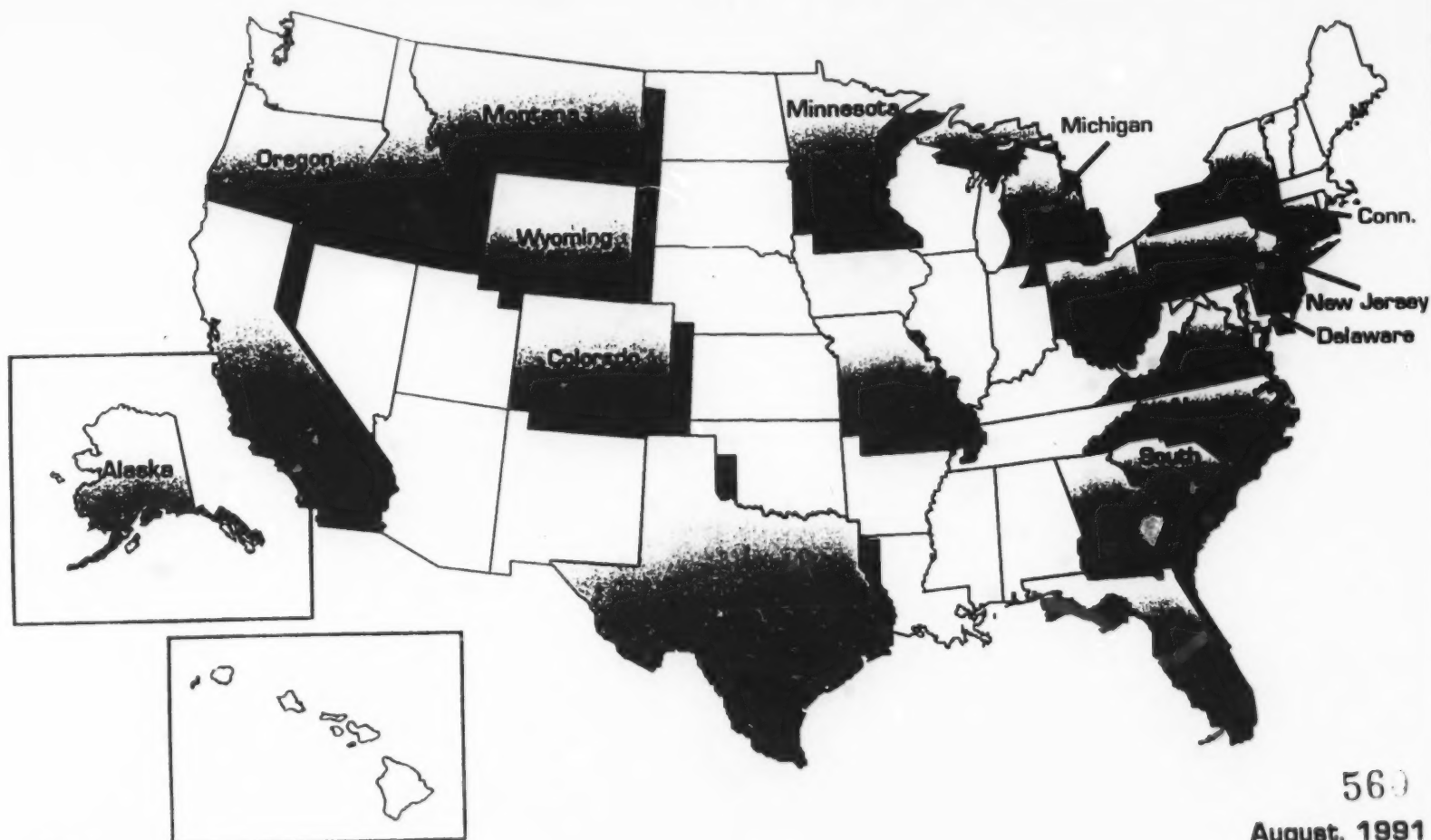
COURSE SUMMARY

IN UTILIZING III, IT IS PARTICULARLY IMPORTANT TO REMEMBER:

- 1. OBTAINING III RECORDS USUALLY REQUIRES TWO INQUIRIES: THE QH INQUIRY AND THE QR RECORD REQUEST.**
- 2. THE NO RECORD RESPONSE TO A III INQUIRY DOES NOT NECESSARILY MEAN THERE IS NO CRIMINAL HISTORY RECORD FOR THE SUBJECT.**
- 3. ADMINISTRATIVE AND CRIMINAL SANCTIONS CAN BE TAKEN AGAINST AGENCIES AND INDIVIDUALS WHO USE III FOR ANY OTHER REASON THAN A LEGITIMATE, OFFICIAL PURPOSE.**

PARTICIPANTS

Interstate Identification Index Program



559

560
August, 1991

5 § 8913

Note 6

claim upon which relief could be granted since U.S. was not proper party to suit for benefits of such type. Director, Edward J. Meyer Memorial Hospital v. Setz, D.C.N.Y. 1977, 433 F.Supp. 323.

Where applicable statutes and regulations could not be read as specifically directing employing federal officials to classify employees as issue as something other than "temporary," "term" or "intermittent" employees, such parties did not have substantive right to be classified as other than "temporary" or "intermittent," so as to have right to monetary equivalent of annual and sick leave benefits, as well as health and life insurance benefits. Anderson v. U.S., 1984, 5 Cl.Ct. 573, affirmed 764 F.2d 849.

7. Removal of action

Where neither federal question nor diversity jurisdiction could be asserted with respect to suit brought by hospital director to claim amounts allegedly owed by federal employee as result of his wife's hospitalization or to employee's third-party claim against national association of letter carriers seeking to recover health benefits, and where concurrent third-party claim against Commission.

§ 8914. Effect of other statutes

Any provision of law outside of this chapter which provides coverage or any other benefit under this chapter to any individuals who (based on their being employed by an entity other than the Government) would not otherwise be eligible for any such coverage or benefit shall not apply with respect to any individual appointed, transferred, or otherwise commencing that type of employment on or after October 1, 1988.

(Added Pub.L. 100-238, Title I, § 108(a)(3)(A), Jan. 8, 1988, 101 Stat. 1747.)

Historical and Statutory Notes

Legislative History. For legislative history and purpose of Pub.L. 100-238, see 1988 U.S. Code Cong. and Adm. News, p. 3217.

SUBPART H—ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

CHAPTER 91—ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Sec.

9101. Criminal history record information for national security purposes.

§ 9101. Criminal history record information for national security purposes

(a) As used in this section:

(1) The term "criminal justice agency" includes Federal, State, and local agencies and means: (A) courts, or (B) a Government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or Executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(2) The term "criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. The term does not include

MENT ORGANIZATION

which resulted in petition for removal of case from Buffalo City Court, was barred by section 2680 of Title 28 because it was based upon misrepresentation, original claim and remaining third-party claim would be remanded to Buffalo City Court for further determination. Director, Edward J. Meyer Memorial Hospital v. Setz, D.C. N.Y. 1977, 433 F.Supp. 323.

8. Review

Federal regulation stating that federal employees' health benefits policy claimant "may" seek review by OPM does not dispense with requirement of exhaustion of administrative remedies. Bateman v. Blue Cross-Blue Shield of Alabama, D.C.Ala. 1984, 579 F.Supp. 363.

The Office of Personnel Management did not act arbitrarily or capriciously when it refused to order carrier to pay benefits pursuant to plan created under this chapter to cover costs incurred by hospitalization of plaintiff's son, since the Office considered relevant factors and did not make a clear error of judgment. Levin v. Connecticut Blue Cross, Inc., D.C.Ill. 1980, 487 F.Supp. 385.

those records of a State or locality sealed pursuant to law from access by State and local criminal justice agencies of that State or locality.

(3) The term "classified information" means information or material designated pursuant to the provisions of a statute or Executive order as requiring protection against unauthorized disclosure for reasons of national security.

(4) The term "State" means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, the Virgin Islands, American Samoa, the Trust Territory of the Pacific Islands, and any other territory or possession of the United States.

(5) The term "local" and "locality" means any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal, or other local government level.

(b)(1) Upon request by the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency or the Federal Bureau of Investigation, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by such department, office, agency or bureau for the purpose of determining eligibility for (A) access to classified information or (B) assignment to or retention in sensitive national security duties. Such a request to a State central criminal history record repository shall be accompanied by the fingerprints of the individual who is the subject of the request if required by State law and if the repository uses the fingerprints in an automated fingerprint identification system. Fees, if any, charged for providing criminal history record information pursuant to this subsection shall not exceed the reasonable cost of providing such information, nor shall they in any event exceed those charged to State or local agencies other than criminal justice agencies for such information.

(2) This subsection shall apply notwithstanding any other provision of law or regulation of any State or of any locality within a State, or any other law of the United States.

(3)(A) Upon request by a State or locality, the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency, or the Federal Bureau of Investigation shall enter into an agreement with such State or locality to indemnify and hold harmless such State or locality, and its officers, employees and agents, from any claim against such State or locality, or its officer, employee or agent, for damages, costs and other monetary loss, whether or not suit is instituted, arising from the disclosure or use by such department, office, agency or bureau of criminal history record information obtained from the State or locality pursuant to this subsection, if the laws of such State or locality, as of the date of enactment of this section, otherwise have the effect of prohibiting the disclosure of such criminal history record information to such department, office, agency or bureau.

(B) When the Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency or the Federal Bureau of Investigation and a State or locality have entered into an agreement described in subparagraph (A), and a claim described in such subparagraph is made against such State or locality, or its officer, employee, or agent, the State or locality shall expeditiously transmit notice of such claim to the Attorney General and to the United States Attorney of the district embracing the place wherein the claim is made, and the United States shall have the opportunity to make all determinations regarding the settlement or defense of such claim.

(c) The Department of Defense, the Department of State, the Office of Personnel Management, the Central Intelligence Agency, or the Federal Bureau of Investigation shall not obtain criminal history record information pursuant to this section unless it has received written consent from the individual under investigation for the release of such information for the purposes set forth in paragraph (b)(1).

(d) Criminal history record information received under this section shall be disclosed or used only for the purposes set forth in paragraph (b)(1) or for national security or criminal justice purposes authorized by law, and such information shall be made available to the individual who is the subject of such information upon request.

(e) The authority provided under this section with respect to the Department of State may be exercised only so long as the Department of State continues to extend to its employees and applicants for employment, at a minimum, those procedural safeguards provided for as part of the security clearance process that were made available, as of May 1, 1987, pursuant to section 163.4 of volume 3 of the Foreign Affairs Manual.

(Added Pub.L. 99-169, Title VIII, § 801(a), Dec. 4, 1985, 99 Stat. 1008, and amended by Pub.L. 99-569, Title IV, § 402(a), Oct. 27, 1986, 100 Stat. 3196; Pub.L. 101-246, Title I, § 114, Feb. 16, 1990, 104 Stat. 22.)

Historical and Statutory Notes

1990 Amendment. Subsec. (b)(1). Pub.L. 101-246, § 114(1), inserted "the Department of State," after "Defense."

Subsec. (b)(3). Pub.L. 101-246, § 114(1), inserted "the Department of State," after "Defense," wherever appearing.

Subsec. (c). Pub.L. 101-246, § 114(1) inserted "the Department of State," after "Defense."

Subsec. (e). Pub.L. 101-246, § 114(2), added subsec. (e).

1986 Amendment. Subsec. (b)(1). Pub.L. 99-569, § 402(a)(1), added reference to the Federal Bureau of Investigation and reference to such bureau.

Subsec. (b)(3)(A). Pub.L. 99-569, § 402(a)(2), added reference to the Federal Bureau of Investigation and references to such bureau wherever appearing.

Subsec. (b)(3)(B). Pub.L. 99-569, § 402(a)(3), added reference to the Federal Bureau of Investigation.

Subsec. (c). Pub.L. 99-569, § 402(a)(4), added reference to the Federal Bureau of Investigation.

Effective Date of 1986 Amendment. Section 402(c) of Pub.L. 99-569 provided that: "The amendments made by this section (amending this section and sections 803(a) of Pub.L. 99-169 set out as a note under this section) shall become effective with respect to any inquiry which begins after the date of enactment of this Act [Oct. 27, 1986] conducted by the Federal Bureau of Investigation for purposes specified in paragraph (b)(1) of section 9101 of title 5, United States Code [subsec. (b)(1) of this section]."

Effective Date. Section 802 of Pub.L. 99-169 provided that: "The amendments made by section 801(a) of this Act (enacting this section), shall become effective with respect to any inquiry which begins after the date of enactment of this Act [Dec. 4, 1985], conducted by the Department of Defense, the Office of Personnel Management, or the Central Intelligence Agency, for the purposes specified in paragraph (b)(1) of section 9101

of title 5, United States Code, as added by this Act [subsec. (b)(1) of this section]."

Extension of Termination Date of Subsection (b)(3) of this Section. Pub.L. 100-453, Title I, § 101(d), Sept. 29, 1988, 102 Stat. 1904, provided that: "The expiration date provided for in section 803(b) of the Intelligence Authorization Act for Fiscal Year 1986 (Public Law 99-169) [set out as a note under this section] shall be extended until December 31, 1989."

Report to Congressional Committees on Effect of Provisions for Indemnification Agreements. Section 803(a) of Pub.L. 99-169 as amended by Pub.L. 99-569, Title IV, § 402(b), Oct. 27, 1986, 100 Stat. 3196 provided that: "Within two years after the date of enactment of this Act [Dec. 4, 1985], the Department of Justice, after consultation with the Department of Defense, the Office of Personnel Management, the Central Intelligence Agency, and the Federal Bureau of Investigation, shall report to the appropriate committees of the Congress concerning the effect of section 9101(b)(3) of title 5, United States Code, as added by this Act [subsec. (b)(3) of this section], including the effect of the absence of indemnification agreements upon States and localities not eligible under section 9101(b)(3) of title 5, United States Code, for such agreements."

Termination Date of Subsection (b)(3) of This Section. Section 803(b) of Pub.L. 99-169 provided that: "(b) Three years after the date of enactment of this Act [Dec. 4, 1985], section 9101(b)(3) of title 5, United States Code [subsec. (b)(3) of this section], shall expire."

Legislative History. For legislative history and purpose of Pub.L. 99-169, see 1985 U.S. Code Cong. and Adm. News, p. 952. See also, Pub.L. 99-569, 1986 U.S. Code Cong. and Adm. News, p. 5327; Pub.L. 101-246, 1990 U.S. Code Cong. and Adm. News, p. 3.

Library References

Reprints 99-60

C.J.S. Records § 36.

QH RESPONSES

Example - Single Positive Response

2L01HEADERXXXX01234.QH.MD1012600.NAM/TEST,T J.SEX/M.RAC/W.DOB/082544.
PUR/C(EOT)

7L01HEADERXXXX01234
MD1012600

THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR
INQUIRY ON NAM/TEST,T J SEX/M RAC/W DOB/082544 PUR/C

NAME	FBI NO.	INQUIRY DATE
TEST,THOMAS JOSEPH	9013000	12/01/90
SEX RAC BIRTH DATE HEIGHT WEIGHT EYES HAIR BIRTH PLACE		
M W 08/25/44 600 185 BLU BRO PENNSYLVANIA		

FINGERPRINT CLASS
23 17 18 19 17
24 18 19 19 17

ALIAS NAMES
TEST,TOM

OTHER	SCARS-MARKS-		
BIRTH DATES	TATTOOS	SOCIAL SECURITY	MISC NUMBERS
11/25/44	TAT R ARM	563-43-5916	AS-563435916

MISC COMMENTS-PA SINGLE-STATE TEST RECORD

IDENTIFICATION DATA UPDATED 11/07/90

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE
FOLLOWING:

PENNSYLVANIA - STATE ID/PA80003048
NEW YORK - STATE ID/NY0000378H - DECEASED

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION
INDEX BY USING THE APPROPRIATE NCIC TRANSACTION.

ATTENTION -- YOUR INQUIRY CONTAINED ONLY THE FIRST INITIAL OF FIRST
NAME. A MORE COMPREHENSIVE RECORD SEARCH MAY BE POSSIBLE IF YOUR
INQUIRY IS RESUBMITTED WITH COMPLETE NAME.
END

Example - Multiple Positive Response

2L01HEADERXXXX01234.QH.MD1012600.NAM/SAMPLE,JOHN.SEX/M.RAC/W.DOB/
122556.PUR/C(EOT)

3L01HEADERXXXX01234
MD1012600

THIS NCIC INTERSTATE IDENTIFICATION INDEX MULTIPLE RESPONSE IS THE
RESULT OF YOUR INQUIRY ON NAM/SAMPLE,JOHN SEX/M RAC/W DOB/122556
PUR/C

NAME	FBI NO.	INQUIRY DATE
SAMPLE,JOHN PATRICK	9015174	12/01/90

#SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE
M	W	12/25/56	601	189	BLU	BRO	MICHIGAN

FINGERPRINT CLASS
PO PM 14 CO 09
01 12 XX 17 62

ALIAS NAMES
SAMPLE,PATRICK

OTHER	SCARS-MARKS-		
BIRTH DATES	TATTOOS	SOCIAL SECURITY	MISC NUMBERS
11/25/56	TAT R ARM	563-43-5916	AS-563435916
10/25/56	TAT CHEST	463-34-8119	AS-88104

MISC COMMENTS-PERSON IS DIABETIC-THIS IS AN FBI TEST RECORD

IDENTIFICATION DATA UPDATED 04/23/84

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE
FOLLOWING:

FLORIDA - STATE ID/FL000000123
FBI - FBI/9015174

END - 1ST NCIC III RECORD OF MULTIPLE RESPONSE

NAME	FBI NO.	INQUIRY DATE
SAMPLE,JAMES	9026285	12/01/90

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE
M	W	12/25/58	511	155	BRO	RED	GEORGIA

FINGERPRINT CLASS
AA TT 21 PM 22
10 51 13 25 02

MISC COMMENTS-THIS IS AN FBI TEST RECORD

IDENTIFICATION DATA UPDATED 04/24/84

Example - Multiple Positive Response (continued)

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE FOLLOWING:

MICHIGAN - STATE ID/MI054321
END - LAST NCIC III RECORD OF MULTIPLE RESPONSE

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION INDEX BY USING THE APPROPRIATE NCIC TRANSACTION.
END

A maximum of 15 records will be provided on-line for a multiple response. In instances where 16 or more records match the QH inquiry, a caveat will be appended to the QH multiple record response that contains the FBI number(s) of the additional matching records.

Example:

END - 15TH NCIC III RECORD OF MULTIPLE RESPONSE

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION INDEX BY USING THE APPROPRIATE NCIC TRANSACTION.

NOTICE: AS A RESULT OF YOUR INQUIRY, THE III PROVIDED A MAXIMUM OF 15 MATCHING RECORDS. TO OBTAIN ADDITIONAL MATCHING RECORD(S), USE A SEPARATE III INQUIRY(S) CONTAINING THE FOLLOWING FBI NUMBER(S):
1234561 1234562 1234563

END

Example - Response When a QH Record Has Been Removed From III as a
Result of Consolidation, Deletion, Expungement, or Subject's
Death

2L01HEADERXXXX01234

MD1012600

THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF
YOUR INQUIRY ON FBI/9015174 PUR/C

RECORD NO LONGER ON FILE - CONSOLIDATED WITH FBI/9026285 120190
END

(or)

RECORD NO LONGER ON FILE - DELETED 120190
END

(or)

RECORD NO LONGER ON FILE - EXPUNGED 120190
END

RECORD NO LONGER ON FILE - DECEASED
PER POLICE DEPARTMENT SUMTER SC 120190
END

Example - "G" Type Response

GL01HEADERXXXX01234

MD1012600

THE FBI IS UNABLE TO PROVIDE A RESPONSE FOR FBI/9030300.
FBI PERSONNEL WILL RESEARCH THE PROBLEM AND YOU WILL BE
ADVISED.
END

GL01HEADERXXXX01234

MD1012600

THE FBI EXPERIENCED A TECHNICAL PROBLEM WHILE PROCESSING YOUR
REQUEST FOR FBI/9015174.
IF YOU DID NOT RECEIVE YOUR RESPONSE,
PLEASE MAKE ANOTHER REQUEST.
END

As appropriate, "FBI/(FBI number)" will be replaced with
"SID/(SID number)." For QH responses, "FBI/(FBI number)" will be
replaced by "NAM/(name)" and the other search fields from the inquiry.

Example - No Response

NL01HEADERXXX01234

MD1012600

NO IDENTIFIABLE RECORD IN THE NCIC INTERSTATE IDENTIFICATION INDEX (III) FOR
NAH/SAMPLE,MICHAEL.SEX/M.RAC/W.DOB/102556

NOTICE — THIS DOES NOT PRECLUDE THE POSSIBLE EXISTENCE OF MATCHING RECORDS IN
LOCAL, STATE, OR FBI IDENTIFICATION DIVISION FILES THAT ARE NOT INDEXED IN THE
NCIC III. IF YOU DESIRE A SEARCH OF THE FBI IDENTIFICATION DIVISION FILES,
A FINGERPRINT CARD SHOULD BE SUBMITTED.
END

Example - Reject

JL01HEADERXXXXX0?76

REJECT HEADER ERROR

Example - "F" Type Response

FLOIHEADERXXXX01234

MD1012600

THIS INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR RECORD REQUEST FOR FBI/9021100. INDIVIDUAL'S RECORD WILL BE COMPLETE WHEN ALL RESPONSES ARE RECEIVED FROM THE FOLLOWING SOURCES EXCEPT FOR THOSE INDICATED AS DECEASED:

FBI - FBI/9021100
NORTH CAROLINA - STATE ID/NC0142658A - DECEASED
TEXAS - STATE ID/TX01346790

AN ADDITIONAL RECORD MAY BE OBTAINED FROM FILES WITHIN YOUR STATE.
END

Example - "-" Type Response

4LOIHEADERXXXX01234

MD1012600

ATN/DET JOHN Q PUBLIC

THIS RECORD IS BASED ONLY ON THE FBI NUMBER IN YOUR REQUEST-9021100. BECAUSE ADDITIONS OR DELETIONS MAY BE MADE AT ANY TIME, A NEW COPY SHOULD BE REQUESTED WHEN NEEDED FOR SUBSEQUENT USE.

- FBI IDENTIFICATION RECORD -

WHEN EXPLANATION OF A CHARGE OR DISPOSITION IS NEEDED, COMMUNICATE DIRECTLY WITH THE AGENCY THAT FURNISHED THE DATA TO THE FBI.

NAME	FBI NO.	DATE REQUESTED
SAMPLE, JOHN PATRICK	9021100	12/01/90

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE
M	W	12/02/50	601	189	BLU	BRO	MICHIGAN

FINGERPRINT CLASS

PO PM 14 CO 09

01 13 XX 17 62

1-ARRESTED OR RECEIVED 10/18/83

AGENCY-FBI BALTIMORE MD (MDFBIBA00)

AGENCY CASE-91-1011 NAME USED-SAMPLE, PATRICK

CHARGE 1-BANK ROBBERY

COURT-

01/15/84 DISPOSITION-CONVICTED

CHARGE-BANK ROBBERY

SENTENCE-10 YEARS SUSPENDED

GUILTY PLEA

Example - "4" Type Response (continued)

```
-----
*           WANTED                               *
*
*   CONFIRM WARRANT STILL OUTSTANDING           *
*
*   AGENCY-DEPT JUST COMM CTR WASHINGTON (DCDOJ02X4) *
*   WANTED-NCIC #W599383830                     *
*   HOTDOG, FRANK T                             *
*   HOMICIDE - WILLFUL KILL-POL OFF-GUN         *
*   CASE #TEST                                  *
*   DATE OF WARRANT 081690                      *
*   NOTIFY DEPT JUST COMM CTR WASHINGTON DIST OF COLUMBIA *
*
*-----
```

ADDITIONAL CRIMINAL HISTORY RECORD INFORMATION IS MAINTAINED BY THE FOLLOWING STATE(S):

NORTH CAROLINA - STATE ID/NC0142658A - DECEASED
TEXAS - STATE ID/TX01346790

THE USE OF THIS RECORD IS REGULATED BY LAW. IT IS PROVIDED FOR OFFICIAL USE ONLY AND MAY BE USED ONLY FOR THE PURPOSE REQUESTED.
END OF RECORD

Example - "E" Type Response

EL01HEADERXXXX01234
MD1012600

THIS INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR RECORD REQUEST FOR FBI/9001100. INDIVIDUAL'S RECORD WILL BE COMPLETE WHEN ALL RESPONSES ARE RECEIVED FROM THE FOLLOWING SOURCES EXCEPT FOR THOSE INDICATED AS DECEASED:

NORTH CAROLINA - STATE ID/NC0142658A - DECEASED
TEXAS - STATE ID/TX01346790

AN ADDITIONAL RECORD MAY BE OBTAINED FROM FILES WITHIN YOUR STATE.
END

Example - "E" Type Response When Requesting Agency's State Repository Maintains the Only Record on the Subject

EL01HEADERXXXX01234
MD1012600

THIS INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR RECORD REQUEST FOR FBI/9007000. THE RECORD MAY BE OBTAINED FROM FILES WITHIN YOUR STATE - THE INTERSTATE IDENTIFICATION INDEX CONTAINS NO ADDITIONAL DATA:
END

Example - "C" Type Response

GL01HEADERXXXX01234

MD1012600

DUE TO A TECHNICAL PROBLEM, THE FBI WAS UNABLE TO PROVIDE A RESPONSE FOR FBI/9015174. YOUR REQUEST WAS RECEIVED AT 2115 EST ON 12/7/90.

PLEASE MAKE ANOTHER REQUEST IF YOU HAVE NOT ALREADY DONE SO.

END

Example - "H" Type Response

HL01HEADERXXXX01234

MD1012600

THIS INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR RECORD REQUEST FOR FBI/9001100. THE NCIC HAS BEEN UNABLE TO NOTIFY THE FOLLOWING BUT WILL CONTINUE TO RETRY:

TEXAS - STATE ID/TX01346790

END

Example - "P" Type Response

PL01HEADERXXXX01234

MD1012600

THIS INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR RECORD REQUEST FOR FBI/9001100. THE NCIC HAS BEEN UNABLE TO NOTIFY THE FOLLOWING AND WILL NO LONGER CONTINUE TO RETRY:

TEXAS - STATE ID/TX01346790

YOUR RECORD REQUEST MAY BE RESUBMITTED IF THE RECORD IS STILL NEEDED.

END

Example - "2" Type Response

2L01HEADERXXXX01234

MD1012600

THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF
YOUR RECORD REQUEST FOR FBI/9015174 PUR/C ATN/DET J Q PUBLIC

RECORD NO LONGER ON FILE - CONSOLIDATED WITH FBI/901283 120190
END

(OR)

RECORD NO LONGER ON FILE - DELETED 120190
END

(OR)

RECORD NO LONGER ON FILE - EXPUNGED 120190
END

(OR)

RECORD NO LONGER ON FILE - DECEASED
PER POLICE DEPARTMENT SUMTER SC 120190
END

Example - "X" Type (No Response)

NL01HEADERXXXX01234

MDBPD0000

NO IDENTIFIABLE RECORD IN THE NCIC INTERSTATE IDENTIFICATION INDEX
(III) FOR FBI/9126285.PUR/C.

NOTICE -- THIS DOES NOT PRECLUDE THE POSSIBLE EXISTENCE OF MATCHING
RECORDS IN LOCAL, STATE, OR FBI IDENTIFICATION DIVISION FILES THAT ARE
NOT INDEXED IN THE NCIC III. IF YOU DESIRE A SEARCH OF THE FBI
IDENTIFICATION DIVISION FILES, A FINGERPRINT CARD SHOULD BE SUBMITTED.
END

Example - "J" Type (Reject)

JL01HEADERXXXX0176

MDBPD0000

REJECT QR.SID/MV8133911.PUR/C.DPT/BALTIMORE CITY PD.ATN/
DET JOHN PUBLIC.BLD/MUNICIPAL BLDG, RM 100.ADR/101 MAIN
ST.CIS/BALTIMORE, MD
FOR THE FOLLOWING REASON(S)

FIELD ERROR SID
MISSING DATA ZIP

END

Example - Positive Response

2L01HEADERXXXX01234.ZR.MD1012600.FBI/9015174.PUR/C(EOT)

5L01HEADERXXXX01234
FL0370100
FBI/9015174 ON FILE

Example - No Response Due to Consolidation, Deletion, Expungement, or
Subject's Death

2L01HEADERXXXX1234
MD1012600
THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF
YOUR INQUIRY ON FBI/9015174 PUR/C

RECORD NO LONGER ON FILE - CONSOLIDATED WITH FBI/901283 120190

(OR)

RECORD NO LONGER ON FILE - DELETED 120190

(OR)

RECORD NO LONGER ON FILE - EXPUNGED 120190

(OR)

RECORD NO LONGER ON FILE - DECEASED
PER POLICE DEPARTMENT SUMTER SC 120190

Example - "G" Type Response

GL01HEADERXXXX01234
MD1012600
THE FBI EXPERIENCED A TECHNICAL PROBLEM WHILE PROCESSING YOUR
REQUEST FOR FBI/9040400. IF YOU DID NOT RECEIVE YOUR
RESPONSE, PLEASE MAKE ANOTHER REQUEST.
END

Example - No Response

NL01HEADERXXXX01234
FL0370100
FBI/9015174 NOT ON FILE

Example - Reject

J101HEADERXXXX0177

REJECT INVALID PUR

570



U.S. Department of Justice
Federal Bureau of Investigation
National Crime Information Center (NCIC)

INTERSTATE IDENTIFICATION INDEX (III)

A SUMMARY

Even though the III Program began in 1983, NCIC users continue to request information about the Program and its operations. This publication is intended to answer those questions most frequently asked.

WHAT RECORDS ARE IN III?

The criminal records of about 15 million people are available. These records represent all people born in 1956 or later with an FBI record, persons born prior to 1956 whose first arrest fingerprint card was submitted to the FBI in 1974 or later, and selected older records converted to the automated systems for certain fugitives and repeat offenders.

WHAT IS THE EXTENT OF STATE PARTICIPATION?

Twenty-two state agencies are responsible for providing about half of the available criminal records. Agencies in all states have direct access to the System.

HOW DO I MAKE A III INQUIRY?

If a person's FBI Number is known from a previous fingerprint identification, use it to make the III inquiry. Use of the FBI Number eliminates receiving multiple record responses.

WHAT RECORDS ARE NOT IN III?

There are no records for individuals who have been arrested but whose fingerprints were not sent to the FBI. Also, there are about 12 million older records that are in the FBI manual files only.

WHAT ABOUT FBI PARTICIPATION?

The FBI provides over six million records for Federal offenders and persons arrested in the 28 states not capable of providing their own criminal arrest data.

WHAT IF THE FBI NUMBER IS UNKNOWN?

If the FBI Number is unknown, the index records can be searched for a matching record by using the name, sex, race, and date of birth or Social Security Number. This type of inquiry may result in more than one matching record for persons with similar names and dates of birth.

NOTE: A positive identification can be made only by comparison of fingerprints. Professional judgement must be used to associate records with individuals based solely on names and descriptors.

Revised 10/10/91

**HOW CAN I USE III TO OBTAIN THE
ACTUAL CRIMINAL RECORD?**

To request a criminal record, the subject's assigned FBI or State Identification Number must be used. These numbers may be obtained from local files when a previous fingerprint card was submitted, or they may be obtained by searching the Index. Criminal records are often received from the FBI and state files within 60 seconds of the request.

**WHY NOT JUST REQUEST AN FBI
IDENTIFICATION RECORD?**

III record responses contain as much or more information than the FBI Identification records. Also, getting information via III is quicker. Since updates and expungements are being applied to the files on a continuous basis, we suggest you request another record each time one is needed. This will ensure that the information you have is up to date.

**FOR WHAT PURPOSES CAN III BE
USED?**

III may be used for official criminal justice purposes, e.g., criminal investigation, risk assessment, bond setting, charging determination, sentencing, and criminal justice employment. Also, plans are being considered to use the System for responding to applicant fingerprint cards.

WHAT USES OF III ARE PROHIBITED?

Any noncriminal justice use of the records is generally prohibited. The only exception is when an applicant fingerprint card is identified with a record by the FBI or a state bureau of identification for an authorized purpose.

CAN I USE A FACSIMILE MACHINE TO TRANSMIT CRIMINAL HISTORY RECORDS?

Yes, providing that both agencies involved have an NCIC Originating Agency Identifier authorized to receive criminal history information. Not all facsimile machines are monitored continually, so it is important to notify the receiving agency by telephone prior to transmitting the information. This will ensure proper retrieval of information and serves to verify the authenticity of the receiving agency.

RECORD-PROVIDING STATES

Alaska	Michigan	Oregon
California	Minnesota	Pennsylvania
Colorado	Missouri	South Carolina
Connecticut	Montana	Texas
Delaware	New Jersey	Virginia
Florida	New York	Wyoming
Georgia	North Carolina	
Idaho	Ohio	